Forensic Services

Svenska Filminstitutet

Projekt Proton

pwc

Svenska Filminstitutet
Att: Anna Serner
Box 27126
102 52 Stockholm

Ulf Sandlund
Director, Forensic Services
E-post: ulf.sandlund@se.pwc.com
Telefon: +46 (0)709 29 36 07

Cecilia Andersson
Assistant Manager, Forensic Services
E-post: cecilia.a.andersson@se.pwc.com
Telefon: +46 (0)709 29 33 20

Stockholm den 12 december 2011

I enlighet med överenskommelse översänder vi avrapportering avseende vår genomgång av säkerhetsfrågor m m.

Med vänlig hälsning

Ulf Sandlund

Innehållsförteckning

Avsnitt 1
Introduktion

Uppdrag, syfte och begränsningar

Den 12 september ombad Svenska Filminstitutet (”SFI”) Öhrlings PricewaterhouseCoopers AB (”PwC”) att göra en genomgång av SFI:s interna hantering av film och därtill kopplade säkerhetsfrågor. Bakgrunden till detta var att SFI har mottagit uppgifter från externa uppgiftslämnare om att otillbörlig hantering skett inom SFI:s nätverk och att SFI:s personal antyddes ha medverkat till att filmer otillbörligen kopierats och tillgängliggjorts för allmänheten. Dessa uppgifter förekommer också i polisanmälan, tillsammans benämnda (”Tredjepartsuppgifterna”).

Det övergripande syftet med vårt arbete har varit att

a) etablera fakta huruvida eventuell vårdslös eller otillbörlig hantering av film kan skett inom SFI och om detta kan kopplas till olika påståenden om SFI eller dess personal i Tredjepartuppgifterna,

b) undersöka om brister funnits (eller alltjämt finns) i teknisk och fysisk hantering av filmer,

c) på basis av iakttagelser i vårt arbete utarbeta rekommendationer om förbättringsåtgärder i SFI:s hantering av film med fokus på fysisk hantering och informationssäkerhet.

Genomfört arbete

Inom ramen för uppdraget har vi utfört flera olika arbetsmoment enligt nedan:

- Omfattande intervjuer med SFI:s personal.
- Genomgång av relevant dokumentation.
- Genomgång av fysisk hantering av film och rutiner för detta.
- Säkring och analys av för genomgången relevant data, bl a loggfiler från IT-system, brandväggsloggar m m.
- Forensisk-teknisk säkring och analys av ett urval datorer vi bedömt vara relevanta för vår genomgång.
- IT – penetrationstestning i syfte att testa säkerhetsbrister i SFI:s nätverk samt utvärdera möjligheterna till att fildela från intern miljö.
- Uppföljning av säkerhetsrelaterade incidenter under uppdragets gång, bland annat kopplade till hyresgäst i Filmhuset.
- Kontakter med Doubletrace (utomstående aktör som har inkommit med information till SFI m m).

Vid sidan av denna avrapportering har vi fortlöpande delat resultaten av vårt arbete med SFI i syfte att snabbare kunna åtgärda uppmärksammade brister i intern kontroll och säkerhetsfrågor.

Tredjepartsuppgifterna - Kontakter mellan Doubletrace och SFI, efterföljande polisanmälan m m

Om Tredjepartsuppgifterna

Den 9 september 2011 upprättade Sveriges Film och TV-Producenter, Sveriges Biografägareförbund och Sveriges Filmuthyrareförening polisanmälan om upphovsrättsbrott, nedan benämnda ”Aktörerna”.

Uppgifterna i polisanmälan gör gällande att olovlig framställning av kopior av filmerna ”Åsa-Nisse Wälkom to Knohult”, ”Flickan som lekte med elden”, ”Kyss mig” och ”Gränsen” skett samt att dessa otillbörligen tillgängliggjorts för allmänheten från SFI:s nätverk och antyder att SFI:s personal kan ha agerat otillbörligt i samband med detta.

Doubletrace, ett företag som vi förstår har anlitats av Aktörerna för att spåra fildelning på Internet, har tillhandahållit information som bilagts polisanmälan och hade dessförinnan haft vissa kontakter med SFI för att förmedla information om den påstådda incidenten.

I vårt arbete med att etablera fakta huruvida eventuell vårdslös eller otillbörlig hantering av film kan ha skett inom SFI har vi särskilt fokuserat på att validera fyra av de påståenden som ingår i Tredjepartsuppgifterna.

Vi har även gjort andra analyser och observationer som inte har direkt koppling till Tredjepartsuppgifterna, men som vi anser är relevanta för att bättre förstå och kunna bedöma bärigheten i påståendena och för att underlätta våra åtaganden i övrigt.

Begränsningar

Begränsningar

Vår genomgång har också varit avgränsad till SFI:s kontrollsfär. Detta innebär bland annat att vi inte haft möjlighet att utreda och analysera aktiviteter genomförda av utomstående och ej heller SFI:s personals privata förehavanden.

I detta har vi ytterligare avgränsat våra urval i vårt arbete utifrån materialitet och risk. Om vi utfört ytterligare åtgärder, exempelvis utgått från ett annat urval kan inte uteslutas att ytterligare förhållanden skulle kunna ha noterats.

Kopior av, eller utdrag ur, detta arbetsutkast till rapport får ej framställas utan vårt skriftliga tillstånd till andra än behöriga representanter för SFI.

Vi har inom ramen för detta uppdrag inte utfört någon revision enligt god revisionssed och lämnar således inget revisionsutlåtande.

Ordlista och definitioner

Benämning	Förklaring
Brandvägg	Programvara och/eller hårdvara som används för att begränsa inkommande och utgående anslutningar från ett nätverk.
Bittorrent	En teknik för fildelning via Internet.
De aktuella filmerna	De filmer som per den 8 november var knutna till alias MEMFiS på Pirate Bay: Åsa Nisse – Wälkom to Knohult, Gränsen, Kronjuvelerna, Kyss mig, Jag saknar dig, Jägarna 2 samt Happy End.
Direct Connect, DC++	En teknik och programvara för fildelning via Internet.
Hubb	Benämningen på en server som används för fildelning via Direct Connect.
IP-nummer	Nätverksadress till en dator eller annan nätverksenhet (t ex brandvägg). IP-numret kan vara externt och exponerat mot Internet, eller internt inom ett lokalt nätverket.
Klient	Generell benämning på en dator i ett nätverk, normalt en arbetsstation eller laptop. Klient kan även referera till en dator som är ansluten till en server, t ex en fildelningsserver.
Master copy	Benämning som används i polisanmälan för att beskriva filmfilerna som Doubletrace identifierat på en dator ansluten via SFI:s nätverk.
(The) Pirate Bay	En populär sökmotor för filer tillgängliga för nedladdning via Bittorrentteknik.
Port	Adress för en specifik anslutning till ett visst IP-nummer. Ofta används en viss port till vissa typer av trafik, exempelvis port 80 för hemsidor.
Protokoll	En uppsättning regler och nyckelord för hur kommunikation över en Internetanslutning skall genomföras.
Subnät	En del av ett nätverk som kan innehålla en grupp av datorer med separata IP-nummer. Vilket subnät en dator tillhör kan utläsas ur IP-numret.
SFI:s kontrollsfär	SFI:s kontrollsfär avser SFI:s egendom, utrustning samt anställd personal.

Ordlista och definitioner (forts.)

Benämning	Förklaring
Telecine	Benämning som används i polisanmälan för att beskriva kvalitet på de påstådda illegala kopiorna samt hur de påstås ha framställts. Telecine-skanner är en utrustning som används för digitalisering av bildmaterial från t ex 35 mm.
Tredjepartsuppgifterna	SFI:s korrespondens med Aktörerna och företaget Doubletrace under augusti och september samt polisanmälan.

Avsnitt 2
Sammanfattande observationer och rekommendationer

Sammanfattning

Otillbörlig hantering av film har ej kunnat knytas till SFI:s kontrollsfär

Vi har inte identifierat några bevis som tyder på att SFI eller dess personal har haft koppling till Tredjepartsuppgifterna. Vi har därmed inte heller kunnat finna stöd för att oegentlig hantering av film skett inom SFI:s kontrollsfär på sätt som antyds i Tredjepartsuppgifterna. Detta gäller såväl påstående om kopiering av film som påstådda tillgängliggörande för allmänheten.

Tredjepartsuppgifterna bedöms vara korrekta ifråga om att fildelning i någon omfattning förefaller ha ägt rum bakom den brandväggslösning och Internetuppkoppling som SFI tillhandahåller för såväl hyresgäster och allmänheten som för SFI:s egna lokala nätverk. När vi har undersökt om det är möjligt att fildela från nätverket har vi lyckats. Vårt tillvägagångssätt skiljer sig dock från den teknik som angivits i påståendena och som används på Pirate Bay. Detta innebär att SFI:s brandvägg inte har blockerat all sorts fildelningstrafik. Att fildelning i någon omfattning förefaller ha ägt rum stöds även av dokument i Tredjepartsuppgifterna som knyter SFI:s IP-nummer för brandväggen till olika påståenden. Det behöver dock inte alls innebära att just SFI:s personal eller utrustning i övrigt kan kopplas till påståendena i Tredjepartsuppgifterna eftersom en del av övrig Internettrafik i Filmhuset, inklusive den för hyresgäster och allmänhet, också passerar SFI:s brandväggslösning. Vi har inte identifierat några bevis som tyder på att SFI eller dess personal har haft koppling till Tredjepartsuppgifterna.

Våra kommentarer i sammandrag om valideringsresultat av påståenden i Tredjepartsuppgifterna framgår i det följande avsnittet.

Brister vid SFI:s hantering av filmer – men också en fråga för branschen

I vårt arbete har vi observerat olika brister i hur filmmaterial har hanterats i Filmhuset. Bristerna innefattar avsaknad av tydliga rutiner likväl som undermålig spårbarhet vid mottagning, intern hantering samt återlämnande av filmmaterial.

Eftersom branschen generellt sett är särskilt sårbar för intrång och upphovsrättsbrott, är vi förvånande att inte en standard etablerats i branschen för säkrare hantering av film och att förväntningar på ansvarsfrågor inte klargjorts. Vi anser att SFI och andra aktörer skulle vinna på att agera mer proaktivt i frågor om hantering av filmmaterial.

Avsnitt 2.1
Sammandrag - valideringsresultat Tredjepartuppgifter

Valideringsresultat – påståenden i Tredjepartsuppgifterna (1/4)

Påstående 1

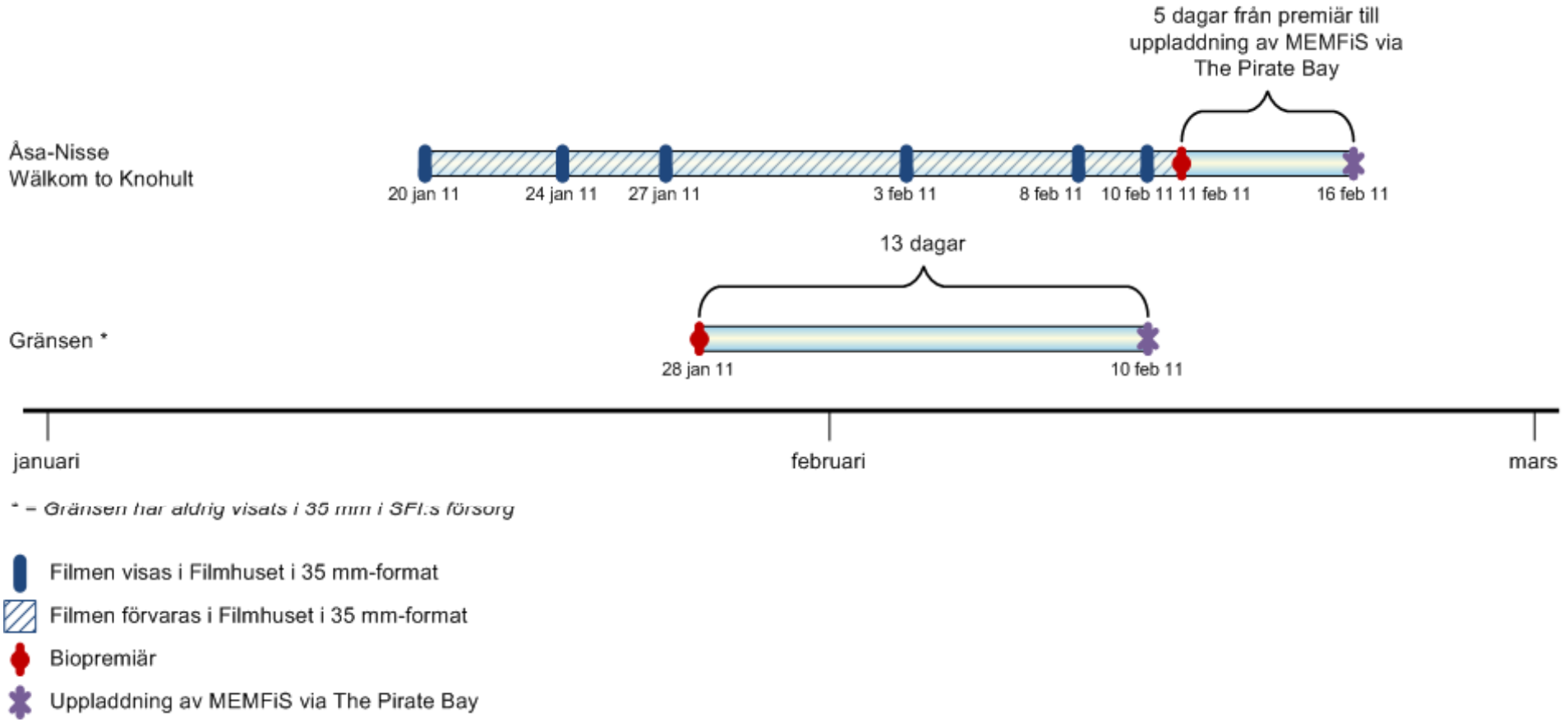
Olovlig framställning av filmerna ”Åsa-Nisse Wälkom to Knohult”, ”Flickan som lekte med elden”, ”Kyss mig”, och ”Gränsen”, samt antydningar om att SFI:s personal kan ha varit involverade i detta. I detta påstås även ”Åsa-Nisse Wälkom to Knohult” och ”Gränsen” vara s k Telecinekopior. [Polisanmälan 2011-09-09]

- Vi har inte identifierat några bevis för att SFI haft den utrustning som krävs för att omvandla 35 mm filmerna till digitalt format, t ex Telecine.
- Inte heller har vi identifierat några bevis för att den av SFI inköpta Telecine-utrustningen funnits i Filmhuset under den tidsperiod som kan utläsas av Tredjepartsuppgifterna, d v s från 20 januari 2011 och framåt.
- Likaså har vi inte heller funnit några belägg för att filmen Gränsen (35 mm) funnits i eller visats i Filmhuset.
- Vi har observerat att de uppladdningar som ser ut att kunna kopplas till signaturen MEMFiS på Pirate Bay synes i samtliga fall ha skett efter premiär. Detta skulle kunna antyda att filmerna kan ha spridits till en vidare krets före uppladdningstillfällena.

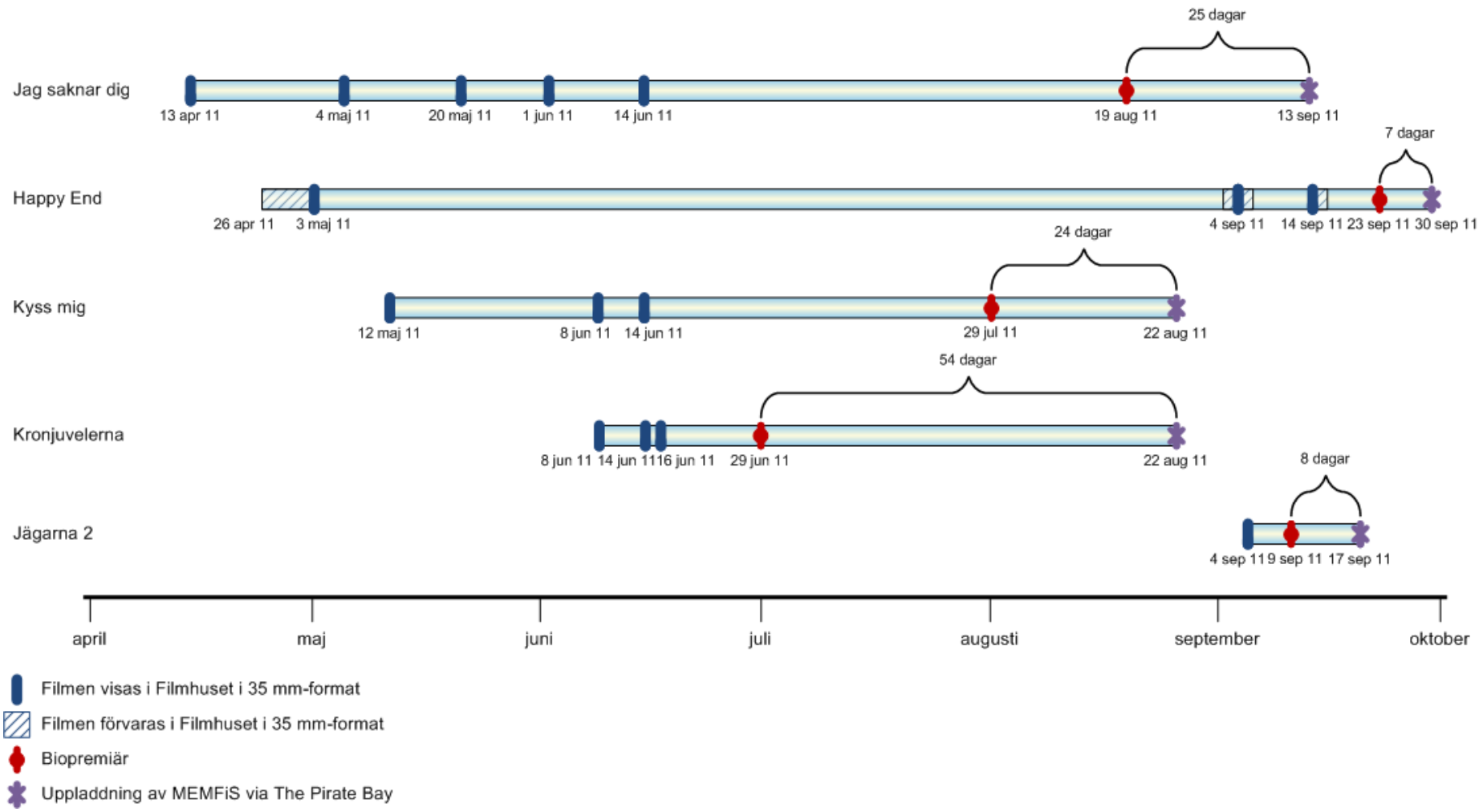
  SFI har visserligen haft brister i den interna kontrollen över mottaget filmmaterial men vi har identifierat omständigheter som talar för att det varit föga sannolikt att fysiskt kopiera 35 mm filmer på sätt som påstås under den aktuella perioden, bland annat:

  - Att flera av de aktuella filmerna, däribland ”Kyss mig”, ”Kronjuvelerna” och ”Jägarna 2”, endast förvarats under kort tid i Filmhuset vilket begränsar möjligheten att någon har hunnit ta med filmmaterial utanför Filmhuset, exempelvis för kopiering.
  - Att producenter i vissa fall närvarat och haft kontroll över filmmaterial vid visningar.
  - Att uppladdning av kopior av de aktuella filmerna, som synes ha laddats upp av alias MEMFiS via Pirate Bay har skett efter filmpremiärer vilket innebär att filmerna varit tillgängliga för en mycket vid krets.

Översikt – premiärer jämfört med visningar i Filmhuset samt uppladdning via The Pirate Bay



Översikt – premiärer jämfört med visningar i Filmhuset samt uppladdning via The Pirate Bay (forts.)



Valideringsresultat - påståenden i Tredjepartsuppgifterna (2/4)

Påstående 2

Att s k ”master copies” av filmerna ”Åsa-Nisse Wälkom to Knohult” och ”Gränsen” enligt Doubletrace ska, via Direct Connect, ha laddats upp från en dator som delvis har varit ansluten via SFI:s nätverk. Doubletrace antyder vidare att den olovliga distributionen kan ha skett från en eller flera infiltratörer bland SFI:s anställda. [Polisanmälan 2011-09-09]

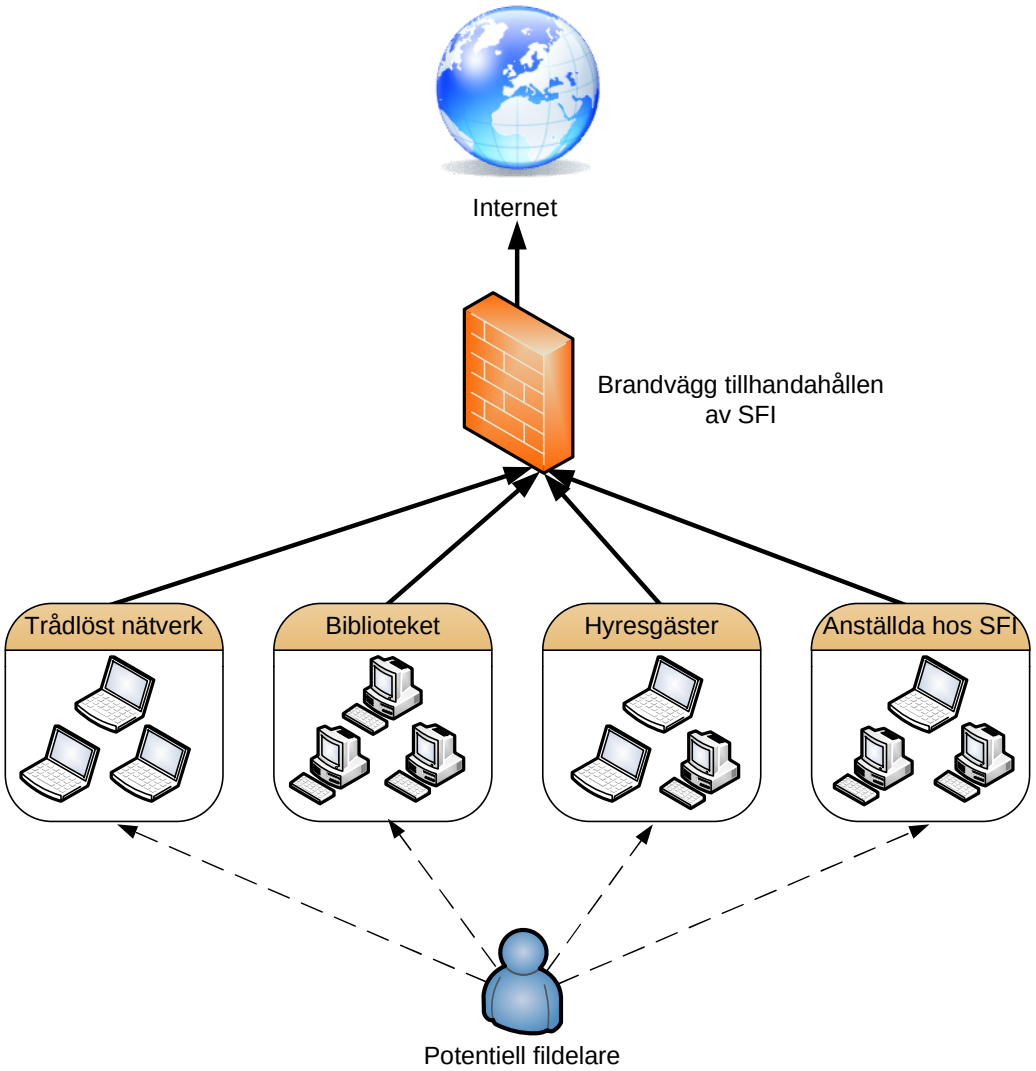
Vi har inledningsvis ställt oss frågan om det varit tekniskt möjligt att distribuera film via SFI:s nätverk på sätt som påstås i Tredjepartsuppgifterna. Av detta skäl har vi bland annat genomfört testning från det öppna trådlösa nätverket till en yttre miljö. D v s undersökt huruvida det var möjligt att fildela bakom SFI:s brandväggslösning till mottagare på utsidan.

- Vid testning från det öppna trådlösa nätverket kunde vi använda en vanlig fildelningsprogramvara (Direct Connect) och fildela till en mottagare på utsidan. Den fildelningsmöjlighet vi identifierade skiljde sig dock åt i förhållande till de muntliga uppgifter vi förstått att Doubletrace lämnat till SFI, nämligen genom att olika portar har använts för överföringen. Detta innebär att vid tiden för vår testning (och dessförinnan) har det varit tekniskt möjligt att fildela och en mottagare på utsidan har alltså kunnat ladda ned material från en dator i Filmhuset som använder sig av SFI:s nätverk.
- Identifierad fildelningsmöjlighet har funnits oberoende av om en fildelare varit tillfällig besökare från allmänheten i Filmhusets cafeteria, agerat från hyresgästernas lokaler eller hanterat detta från SFI:s s k subnät, eftersom alla ovanstående verkar bakom SFI:s brandvägg och därmed tidigare har haft samma externa IP-adress mot Internet. Filmfiler kan alltså ha funnits i IT-verktyg som inte ingår i SFI:s kontrollsfär.

Utöver detta har vi bland annat säkrat och analyserat mycket stora volymer med brandväggsloggar. På basis av resultatet från detta arbete och Tredjepartsuppgifterna har vi genomfört IT-forensisk säkring och analys av sammanlagt 10 stycken datorer som finns inom SFI:s kontrollsfär, vilka vi bedömt vara relevanta för vår genomgång.

- Vi har inte identifierat några bevis för att de IT-verktyg och den metadata vi valt att säkra och analysera innehåller uppgifter som kan sättas i samband med Tredjepartsuppgifterna.
- Vi har i sig kunnat identifiera olämpliga beteenden som strider mot SFI:s regler om användning av IT-verktyg vid genomgång av datorerna, men bedömt att detta överhuvudtaget inte har någon koppling till Tredjepartsuppgifterna.

Illustration – grupper av användare som kunnat agera bakom SFI:s brandväggslösning



Valideringsresultat - påståenden i Tredjepartsuppgifterna (3/4)

Påstående 3

Att filmen Åsa-Nisse Wälkom to Knohult" enligt Doubletrace påståenden i Tredjepartsuppgifterna tillgängliggjorts på Pirate Bay via SFI:s IP-adress av alias MEMFiS den 16 februari 2011. [E-postkommunikation mellan Doubletrace och SFI den 28 augusti 2011]

- Vi har hittills inte identifierat några bevis för att "Åsa Nisse Wälkom till Knohult" och ej heller övriga filmer knutna till alias MEMFiS tillgängliggjorts på Pirate Bay via SFI:s nätverk. Vi har därför inte heller kunnat hitta några kopplingar till att SFI:s personal eller de IT-verktyg som står under SFI:s kontrollsfär kan sättas i samband med påståendena i Tredjepartsuppgifterna.

  Utöver detta har vi också genomfört analyser och observationer som är relevanta att beakta i detta:

  - SFI:s brandväggslösning innehåller en säkerhetsmodul- IPS – vilken bland annat blockerar bittorrenttrafik, d v s den standard som används vid fildelning på Pirate Bay. SFI har, enligt uppgifter från SFI:s IT-avdelning, för sin IPS-modul tillämpat blockering av bittorrenttrafik alltsedan utgången av 2010. Bittorrent är en annan teknik än den som vi har använt i vår testning där vi har identifierat en fildelningsmöjlighet.
  - Under vår genomgång den 23 september 2011 har försök till fildelning från en hyresgästs lokaler i Filmhuset uppmärksammats och förhindrats. Anledningen till att detta uppmärksammades av SFI var att IPS-modulen larmade och stoppade misstänkt bittorrenttrafik. Detta är ett exempel som visar att blockering av bittorrenttrafik fungerat. De individer som kunde sättas i samband med detta utgjordes av s k frilansare inhyrda av hyresgästen.
  - SFI:s anställda är förhindrade att installera programvaror på eget initiativ på de datorer som ingår i SFI:s kontrollsfär. All programinstallation sker via SFI:s IT-avdelning, vilket förhindrar eller i vart fall försvårar att icke tillåtna programvaror installeras, t e x programvara för fildelning.
  - Vi har undersökt trafik som skett över SFI:s brandväggslösning till det IP-nummer som kan kopplas till Pirate Bay, bland annat under perioden 9-18 februari. Till skillnad från bittorrenttrafik blockeras alltså inte själva besöken på hemsidor, exempelvis Pirate Bay. I samband med detta identifierades 4 stycken IP-nummer från det öppna trådlösa nätverket i Filmhuset, d v s vare sig SFI:s subnät eller subnät tillhöriga hyresgästerna kunde sättas i samband med detta. Eftersom ingen metadata (loggar) sparas för anslutna datorer till SFI:s trådlösa nätverk är det inte möjligt att spåra detta vidare till specifika datorer.

Valideringsresultat - påståenden i Tredjepartsuppgifterna (4/4)

Påstående 4

Att en dator har varit aktiv på Direct Connect under kortare tidsperioder från SFI:s IP-adress under ca 3 veckor från den 14 juni till och med 8 juli 2011. Under samma tidsperioder säger sig Doubletrace ha laddat ner delar av filmen ”Åsa-Nisse Wälkom to Knohult” från sagda dator. (Doubletrace indikerar endast att viss dator har varit aktiv / inaktiv vid fyra angivna tider per dygn under de 3 veckorna). [E-postkommunikation mellan Doubletrace och SFI den 31 augusti 2011]

- Vi har hittills inte identifierat några bevis för att de IT-verktyg som finns hos SFI varit anslutna på sätt som påstått s i Tredjepartsuppgifterna.

  Vid våra analyser framkom följande:

  - Vid vår genomgång har vi testat bärigheten i Tredjepartsuppgifterna ifråga om att viss dator varit aktiv från SFI:s nätverk under vid angivna tidpunkter under perioden 14 juni till 8 juli 2011. Enbart under denna period förekommer cirka 15 miljoner rader med brandväggsloggar. Vi valde att testa hälften av de tidpunkter som Doubletrace uppgett att viss dator varit aktiv i SFI:s nätverk och avgränsade vårt tidsfönster till +/- 30 minuter. I detta identifierade vi att de största trafikvolymerna under tidfönstren kunde kopplas till olika s k subnät som ligger utanför SFI:s kontrollsfär, i huvudsak öppna trådlösa nätverket och olika subnät för hyresgäster.
  - För att närmare kunna urskilja förekomst om eventuell otillbörlig trafik kan finnas bland SFI:s brandväggsloggar fordras uppgifter om aktuella trafikdestinationer (mottagarens IP-adress utanför brandväggslösningen) eller i vart fall exakta tidpunkter för när anslutningar skett och uppmätts. Vi (och även SFI:s IT-avdelning) har förgäves efterfrågat dessa uppgifter hos Doubletrace. Avsaknaden av dessa uppgifter har medfört att fildelningstrafik som inte blockeras av brandväggslösningen är svår att särskilja från övrig godkänd trafik. Resultatet av detta är att vårt analysarbete fördröjts, och väl så viktigt - att Tredjepartsuppgifterna om tidpunkter och externa IP-nummer i denna del hittills inte kunnat valideras.
  - Doubletrace har lämnat uppgifter till SFI om att viss dator i SFI:s nätvärk varit ansluten vid 24 olika tidpunkter under perioden 14 juni till 8 juli 2011. Den 27 oktober 2011 har Doubletrace för oss uppgett att tidigare lämnad information om dessa tidpunkter kan betrakta som osäkra. Detta gör att vi ställer oss frågande till om de uppgifter Doubletrace har lämnat är korrekta eller inte.

Intern hantering av film samt informationssäkerhet

Brister i fysisk hantering av film

Det finns brister i hur filmmaterial har hanterats i Filmhuset. Det saknas tydliga riktlinjer för hur filmer ska hanteras och förvaras när de har mottagits inför en filmvisning. Det finns även brister gällande dokumentation och spårbarhet av hantering av filmmaterial. För de aktuella filmerna finns det bland annat ingen dokumentation eller kvittens som styrker när SFI har mottagit respektive återlämnat filmmaterialet. Det saknas dessutom spårbarhet om vilka som har hanterat filmmaterialet internt under tiden när SFI har haft filmmaterialet i Filmhuset.

Detta gäller SFI:s hantering av såväl 35 mm film som övriga format, exempelvis DVD som erhålls från producenter eller distributörer.

Brister i hantering och kravställning mot andra aktörer i Filmhuset, hyresgäster m fl

SFI har inte ställt krav på andra aktörer i Filmhuset (hyresgäster m fl) om villkor och ansvar för hur dessa får använda SFI:s nätverk. SFI har i dagsläget en bristande kontroll över hur detta sker. Det finns t ex hyresgäster i Filmhuset som använder egen utrustning för att sätta upp egna lösenordsskyddade trådlösa nätverk.

Informationssäkerhet

Under vårt analysarbete och våra penetrationstester har vi identifierat brister i SFI:s IT-säkerhetsmiljö. Dessa avser bland annat att brandväggen inte stoppade viss typ av fildelningstrafik, bristande spårbarhet i brandväggsloggar och tilldelning av IP-nummer.

Avsnitt 2.2
Rekommendationer

Rekommendationer

Filmhantering

Vi rekommenderar att SFI ser över och stramar upp ansvar, processer och säkerhet för hantering och visning av film. Vissa förbättringsåtgärder har skett sedan vi inledde vårt arbete, men vi anser också att det finns ett värde i att se över arbetssätt i ett bredare perspektiv. SFI skulle bland annat kunna utvärdera om inte alternativa tekniska plattformar kan erbjuda en väsentligt större grad av säkerhet och därmed uppnå en mer stringent fysisk hantering. I detta är det också självklart mycket betydelsefullt att berörda aktörer och upphovsrättsinnehavare engageras i arbetet.

Till dess att en mer säker hantering uppnåtts bör SFI utarbeta och dokumentera riktlinjer och rutiner för hantering av filmmaterial som erhålls av producenter/filmbolag. SFI bör även noga och regelbundet följa upp för att kontrollera att filmmaterial hanteras på ett säkert och spårbart sätt och i detta även se över och om möjligt ytterligare begränsa åtkomst till det utrymme där SFI förvarar filmmaterial. SFI bör i detta även se över och klargöra förväntningar och ansvarsfrågor gentemot branschaktörer och upphovsrättsinnehavare.

Externa aktörer i Filmhuset utanför SFI:s kontrollsfär

Vi rekommenderar att SFI tar fram och klargör vilka krav på uppförande och användning som ställs på användare av nätverket i Filmhuset. Det bör finns tydliga krav och riktlinjer för hyresgäster och m f l, exempelvis användare av det öppna trådlösa nätverket. SFI har en befintlig IT-policy som gäller för SFI:s anställda, men krav och förväntningar på användning och ansvarsavgränsningar saknas för andra aktörer som rör sig i Filmhuset, framför allt hyresgäster.

IT-säkerhet / öppenhet - riskavvägningar

Vi rekommenderar att SFI ser över sin IT-miljö för att ytterligare införa säkerhetsåtgärder. Vissa skärpta säkerhetsåtgärder har genomförts av SFI:s IT-avdelning, bland annat s k segmentering av brandväggs-lösning m m. Vi rekommenderar också att SFI gör regelbunden översyn av sin brandväggskonfiguration och i detta även låter genomföra oberoende penetrationstester.

SFI bör även överväga att bedöma vilka risker och konsekvenser en fortsatt öppen och anonym användning av nätverket kan innebära. De identifierade riskerna bör balanseras mot fördelarna med öppenhet vid användning av nätverket. Vi rekommenderar som ett minimum att SFI överväger om inte vissa webbsidor eller ytterligare tjänster ska blockeras. Ett annan grundläggande åtgärd är att SFI låter se över sin IT-säkerhetspolicy och i vilken mån utbildningsinsatser kan fordras för att bättre klargöra vilka förväntningar som gäller. Datorer och andra IT-verktyg som står under SFI:s kontrollsfär bör också regelbundet genomsökas i syfte att detektera mjukvara och annat som skulle kunna facilitera eller medföra intrång i upphovsrättsligt skyddat material.

Avsnitt 3
Detaljerade observationer

Avsnitt 3.1
Har film kunnat kopierats hos SFI?

Filmhantering och utrustning för kopiering

Om fysisk filmhantering

SFI har flera olika avdelningar som ibland tar emot filmmaterial innan filmerna har haft premiär. Det är bl a inför förhandsvisningar som anordnas i Filmhuset och till Utlandsenheten respektive avdelningen som hanterar lanseringsstöd i Sverige. Utlandsenheten och lanseringsstöd tar ofta emot filmmaterial på DVD för att lansera dessa utomlands eller ge filmer distributionsstöd. Filmarkivet tar även emot säkerhetskopior av filmmaterial, ibland även innan premiär. Detta utgörs av inter-positiv och negativ vilket inte utgör visningsmaterial.

Vid filmvisningar av förhandsmaterial sker normalt leveransen av film till SFI från producentbolag kort före visning. Återlämning sker efter visning. Filmerna anländer till SFI och återlämnas till producentbolagen, oftast via bud. Logg för mottagning, intern hantering och återlämnande fördes inte i samband med att vi initierade vår genomgång.

Logistik och säkerhet vid filmer som omfattas av Tredjepartsuppgifter

Vi har erhållit en beskrivning av SFI när de aktuella filmerna har visats eller förvarats i Filmhuset. Det saknas exakt spårbarhet kring hantering av filmerna. Vi har dock inte funnit något som motsäger den beskrivning som SFI redovisat. I övrigt har vi noterat att:

- Sammanlagt 6 av de 7 filmerna som förefaller ha laddats upp på Pirate Bay av alias MEMFiS har visats vid ett eller flera tillfällen hos SFI. SFI har informerat oss om att filmen Gränsen aldrig visats i SFI:s försorg och att just detta filmmaterial överhuvudtaget inte heller varit i SFI:s förvar i 35 mm format. Utlandsenheten har dock erhållit en ofärdig version av Gränsen på DVD.
- Filmen Åsa-Nisse Wälkom to Knohult har dock funnits under en längre period hos SFI i 35 mm-format.
- Utlandsenheten respektive avdelningen för lansering av film i Sverige har endast erhållit tre av de aktuella filmerna som färdig version på DVD innan premiär. Dessa är Kyss mig, Jag saknar dig och Happy End.
- SFI kan även ha erhållit ofärdigt filmmaterial på DVD eller visat ofärdigt filmmaterial före premiär men detta har uppgetts vara i ej färdigställt skick, t ex ej färdig ljussättning eller utan sluttexter.

Till maskinrummet har en krets på mer än 10 personer haft nycklar och därmed fysisk möjlighet till åtkomst. Dessa utgörs av maskinisterna, chefer på Filminstitutet, personal på IT- och fastighetsavdelningen, personal på Filmarkivet samt väktare och städpersonal. Användning av vanliga nycklar möjliggör inte spårbarhet om vem som har passerat till- eller från maskinrummet.

Vi har noterat att de aktuella filmerna inte varit inlåsta i säkerhetsskåp, trots att detta funnits tillgängligt.

Efter att vår genomgång initierades har SFI påbörjat arbete med att ersätta befintliga lås till maskinrummet som framgent möjliggör spårbarhet. Detta arbete beräknas enligt uppgift från SFI vara klart den 12 december.

Utlandsenheten respektive avdelningen för lansering av film i Sverige har uppgett att de haft DVD inlåsta i skåp vid sina arbetsplatser när de själva inte har varit i Filmhuset.

Filmhantering och utrustning för kopiering (forts.)

Kopieringsutrustning

Vi har inte identifierat några bevis att SFI har haft den utrustning som krävs för att omvandla filmerna från 35 mm format till digitalt format. SFI har tidigare köpt in Telecineutrustning, vilken enligt SFI har levererats till Filmarkivet i Grängesberg (numera tillhörande Kungliga biblioteket). Vi har heller inte funnit några bevis på att den Telecineutrustningen har varit utlånad till SFI under den aktuella perioden som omfattas av Tredjepartsuppgifterna.

Det ska i sammanhanget beaktas att flera av de aktuella filmerna i 35 mm-format endast förvarats en kort tid i Filmhuset vilket begränsar möjligheten att någon skulle ha hunnit med att ta med sig filmmaterial utanför Filmhuset, exempelvis för att kopiera materialet. Dessutom har vi goda skäl att anta att producenterna i vissa fall haft kontroll över filmmaterialet då de personligen har lämnat filmmaterialet till SFI och bevakat det från SFI:s maskinrum vid visningar.

PwC kommentar

Baserat på vår genomgång bedömer vi det som föga sannolikt att fysisk kopiering skulle ha skett med SFI:s utrustning i SFI:s lokaler. Vi kan av naturliga skäl inte utesluta att kopiering skulle kunna ha skett utanför SFI:s lokaler och utanför SFI:s kontroll.

Det finns också andra omständigheter som dessutom talar för att kopiering skulle kunna ha skett hos utomstående. Dessa utvecklas nedan.

De aktuella filmerna - tillgängliga på Pirate Bay

Uppladdning på Pirate Bay i förhållande till tid för premiärer m m

Vi har observerat att de uppladdningar som ser ut att kunna kopplas till signaturen MEMFiS på Pirate Bay synes i samtliga fall ha skett efter premiär. Detta skulle kunna antyda att filmerna kan ha spridits till en vidare krets (och möjliggjort konvertering eller filmning med videokamera) före uppladdningstillfällena. Uppladdningsloggarna med tillhörande tidsstämplar på Pirate Bay kan vi av naturliga skäl inte undersöka.

Vi har inte haft möjlighet att genomföra teknisk audiovisuella undersökningar av de tillgängliga versionerna på Pirate Bay, bland annat eftersom vi inte kan få tillgång till detta material på laglig väg. En sådan undersökning skulle kunna bidra till att bättre bedöma ursprung m m.

I avsnitt 2.1 illustreras när de aktuella filmerna har förhandsvisats i Filmhuset, ställt i relation till tidpunkter för premiärer, och tidigaste kända uppladdningstidpunkter med signaturen MEMFiS på Pirate Bay. Denna jämförelse visar bland annat att premiärer skett för samtliga aktuella filmer före tidigaste kända uppladdningstidpunkt på Pirate Bay.

PwC kommentar

Detta tyder på att de aktuella filmerna rimligen borde ha varit spridda till en mycket stor krets före det att uppladdningar skett på Pirate Bay. Detta kan i sin tur ha medfört att de aktuella filmerna kan ha kopierats (och senare laddats upp på Pirate Bay) helt utanför SFI:s kontrollsfär.

Avsnitt 3.2
Har film kunnat distribueras från SFI?

Tillträde till lokaler och IT infrastruktur

Andra aktörer i Filmhuset

Förutom SFI finns det andra aktörer som huserar i Filmhuset. Bland annat driver SFI ett öppet bibliotek samt hyr ut lokaler till organisationer inom filmbranschen, restaurang och café där allmänheten kan röra sig fritt.

Det är inte bara SFI:s personal som har haft möjlighet att använda sig av SFI:s Internetåtkomst och på det sättet kunnat använda Internet med SFI:s IP-nummer. Även externa aktörer i Filmhuset, exempelvis användare av det öppna trådlösa nätverket eller hyresgästerna har använt Internet via den centrala brandväggen – allt bakom SFI:s IP-adress (193.10.144.66). För en extern observatör utanför SFI:s brandvägg framstår all Internettrafik att ha sitt ursprung från SFI, oavsett om användare utgörs av tillfälliga cafégäster, arbetar hos SFI, eller är hyresgäster.

Kontrollmiljöproblem

SFI har inte ställt krav på andra aktörer i Filmhuset (hyresgäster m fl) om villkoren för hur dessa får använda SFI:s nätverk. SFI har exempelvis tecknat hyresavtal där det endast framgår att Internet ingår. Inga krav eller villkor för användning av SFI:s nätverk beskrivs således i hyresavtalen. SFI har i dagsläget en mycket begränsad kontroll över hur hyresgäster och andra externa aktörer i Filmhuset använder SFI:s nätverk.

SFI har dock vissa möjligheter att identifiera källan för specifik Internettrafik då det är synligt för IT-avdelningen i vilket subnät de olika anslutna klienterna har befunnit sig i nätverket. All Internettrafik som härrör från användarna i de olika subnäten passerar samma brandvägg och har samma IP-nummer.

Parallellt med vårt arbete har SFI:s IT-avdelning, med början från 17 oktober 2011, segmenterat brandväggen vilket medför att varje subnät numera har olika externa IP-adresser. Detta hindrar inte i sig hur Internet kan användas, men aktiviteter och trafik kan numera spåras till olika subnät, d v s till hyresgäster o s v.

Förutom att all trafik från SFI:s nätverk tidigare har haft en (1) extern IP-adress har det funnits flera brister i spårbarhet och i själva brandväggslösningen. I samband med att vi initierade säkring av data framkom att historik över vilka interna IP-adresser som har delats ut till klienter, på samtliga subnät med undantag för SFI:s egna subnät, inte fanns bevarade.

Analys av brandväggsloggar

Erhållna och analyserade loggar

Vi har som en del i vår utredning tagit del av bl a loggfiler från SFI:s brandvägg. Dessa loggar innehåller information om Internettrafik som passerat eller blockerats mellan det interna nätverket och Internet. Analyser har gjorts utifrån loggar för perioden 30 maj - 15 september, med särskilt fokus på 14 juni – 8 juli 2011 vilket utgör den tidsperiod som Doubletrace redovisat för när påstådd dator har varit aktiv och ansluten via SFI:s nätverk. Vi har även erhållit och analyserat loggfiler för perioden 9 - 18 februari 2011 vilket är den period då filmerna Åsa-Nisse Wälkom till Knohult samt Gränsen först blev tillgängliga på Pirate Bay. Sammanlagt har vi hittills inhämtat 92,4 miljoner loggrader.

Från och med vecka 44 arbetar SFI:s IT-avdelning också med att exportera brandväggsloggar i närtid, 15 september – 6 november 2011. Denna data säkras eftersom Doubletrace för oss indikerat att det kan har skett otillbörliga aktiviteter i nutid. Doubletrace har dock inte försett oss med ytterligare information om detta.

Omfattande mängd brandväggsloggar har varit i fokus för vår analys. Till höger illustreras den trafik som är från det interna nätverket under perioden 30 maj till den 15 september 2011. Bilden illustrerar antalet loggrader som härrör till de olika användargrupperna. Tabellen visar enbart loggrader för utgående trafik mot Internet från det interna nätverket i Filmhuset. Det inkluderas därmed inte loggrader från extern trafik eller interna anrop.

Trafik från interna nätverket under perioden 30 maj - 15 september 2011

Användare	Andel loggrader	Antal miljoner loggrader
SFI	25,9%	4,0
Hyresgäster	24,9%	3,8
Öppet WLAN	19,1%	2,9
Biblioteket	11,2%	1,7
Stiftelsen Ingmar Bergman	4,2%	0,6
Övrigt	14,6%	2,2
	100,0%	**15,3**

Källa: Brandväggsloggar

Analys av brandväggsloggar (forts.)

Exempel på genomförda analyser

Analysen av brandväggsloggar har fokuserats på att hitta avvikande mönster i Internettrafiken, t ex IP-nummer som varit aktiva under samtliga tidsfönster som har angetts av Doubletrace, eller anslutningar som skett mot avvikande portar eller destinationer. Vi har bl a analyserat de s k klienter som haft störst mängd trafik, samt sådana som står för den största andelen blockerad trafik.

Utifrån offentliga listor på hubbar för Direct Connect har vi genomfört analyser av trafik mot drygt 2000 IP-nummer där en Direct Connect-hubb finns eller kan ha funnits.

Vi har också analyserat webbtrafik till ett flertal välkända Bittorrent-sidor, se tabell till höger. Detta har resulterat i att totalt 27 IP-nummer som kan associeras med besök på hemsidor för fildelning via Bittorrent identifierats 30 maj – 15 september 2011. Utöver detta har ytterligare fyra IP-nummer i det öppna trådlösa nätverket besökt Pirate Bay under perioden 9-18 februari 2011.

De tre IP-nummer som finns inom SFI:s subnät har knutits mot datorer och användare. Därefter har vi genomfört en forensisk-teknisk säkring och analys av aktuella användares datorer. Då vi endast haft tillgång till datorer tillhörande SFI har analys av övriga datorer, utanför SFI:s kontroll, ej kunnat genomföras.

IP-nummer som besökt Bittorrentsiter
30 maj – 15 september 2011

	SFI	Stiftelsen Ingmar Bergman	Hyresgästerna	Biblioteket	WLAN	Rotebro
The Pirate Bay	3	-	3	2	12	-
BT Junkie	-	-	1	-	2	-
Mininova	-	-	-	-	1	-
Torrentreactor	-	-	-	-	-	-
Isohunt	-	-	1	-	-	-
Dreamseed	-	-	-	-	-	-
Tankafetast	-	-	1	-	1	-
Totalt	**3**	**-**	**6**	**2**	**16**	**-**

Källa: Brandväggsloggar

Forensisk-teknisk säkring ett urval av SFI:s datorer

Vi har genomfört en forensisk-teknisk säkring och analys av ett urval av datorer använda av bl a initialt antydda personer av Doubletrace samt ytterligare fyra datorer som har identifierats efter analys av brandväggsloggar.

Iakttagelser från detta arbete visar att flera av datorerna har använts på ett sådant sätt som strider mot SFI:s IT-policy men förefaller inte ha direkt koppling till uppgifter i polisanmälan och anklagelserna i övrigt.

På en dator har vi identifierat länkar till filer som har funnits på ett externt media (t ex USB-minne) och som har varit namngivna enligt en namnstandard som ofta används vid fildelning.

Ytterligare två datorer har identifieras ha besökt Pirate Bay:s hemsida och har därför genomgått forensisk-teknisk undersökning. Användaren av en av dessa datorer har även haft ytterligare en dator som har analyserats på samma sätt.

På denna dator har fildelningsprogrammet Azureus tidigare varit installerat och det finns även spår av tidigare raderade favoriter som länkar till bittorrentsidor på Internet, såsom The Pirate Bay, Mininova samt Torrentreactor. Användaren av den här datorn har kunnat installera program på den datorn. Enligt IT-avdelningen har detta utgjort ett undantag från deras regler om att användarna inte ska ha behörighet att installera programvara på datorerna.

Av de sammanlagt 10 genomsökta datorerna har inga spår av de aktuella filmerna hittats trots en omfattande analys av filfragment, återskapade filer m m. Vi har inte heller identifierat någon koppling till alias MEMFiS.

Kommentarer

Som ovan redogjorts har det varit möjligt att använda sig av en fildelningsprogramvara utan att SFI:s brandvägg har blockerat trafiken. Eftersom brandväggen inte har blockerat trafik för vissa använda protokoll har denna trafik loggats som accepterad trafik, vilket gör sådan fildelningstrafik svår att särskilja från övrig godkänd trafik. Det finns också exempel på när fildelningstrafik har blockerats.

Under vårt arbete inträffade en incident där SFI:s IT-avdelning uppmärksammade att brandväggen blockerade fildelningstrafik vilken kunde identifieras till en tillfällig hyresgäst. Personal från SFI:s IT-avdelning besökte lokalerna och upptäckte i samband med detta flera datorer med fildelningsprogramvara. Representanter från hyresgästen har därefter för oss uppgett att incidenten kunde knytas till (av hyresgästen) inhyrda frilansare med egna datorer med fildelningsprogram.

Hyresgästen är tillika medlem i Film & TV Producenterna, d v s en av de organisationer som undertecknat polisanmälan mot SFI.

Sammantaget kan vi inte utesluta att fildelning har skett ifrån SFI:s nätverk men mängden av data försvårar analysen av brandväggsloggar. Vi har dock genomfört ett omfattande arbete för att identifiera trafikmönster som skulle kunna sättas i samband med Tredjepartsuppgifterna.

Under arbetets gång har vi haft upprepade, och tyvärr resultatlösa, kontakter med Doubletrace för att få tillgång till information som skulle kunna ha påskyndat och underlättat vårt arbete. Se även avsnitt 3.3 nedan om diskussioner med Doubletrace.

Avsnitt 3.3
Om informationsutbyte med Doubletrace

Om informationsutbyte med Doubletrace

Alltsedan 11 oktober 2011 har vi haft kontakter med Doubletrace i syfte att bättre förstå de uppgifter som förekommer i Tredjepartsuppgifterna och därigenom underlätta och påskynda vårt arbete. Den 12 oktober 2011 översände vi några frågor om tekniska detaljer vilka Doubletrace rimligen enkelt borde kunna ha besvarat mot bakgrund av de uppgifter de tidigare redovisat i Tredjepartsuppgifterna. Därefter har Doubletrace vid olika tillfällen signalerat osäkerhet huruvida man har kvar den av oss efterfrågade informationen.

Den 24 oktober 2011 upptogs diskussionen på nytt varvid Doubletrace fordrade att PwC ingår sekretessavtal innan de kan dela med sig av någon ytterligare information. Efter hand har Doubletrace framställt önskemål om ett bredare och ömsesidigt informationsutbyte. Av detta skäl har vi tyvärr inte kunnat acceptera att ingå ett sådant avtal eftersom detta potentiellt skulle kunna strida mot villkoren för vårt uppdrag hos SFI.

Om vi skulle ha fått tillgång till efterfrågade uppgifter hade vi snabbt kunna identifiera eventuella kopplingar mot intern datatrafik hos SFI och därmed lättare kunna bedöma och validera bärigheten i Tredjepartsuppgifterna.

Om Doubletrace fortfarande önskar förmedla svar på ställda frågor och annan eventuell information har vi förklarat oss öppna att ta emot denna.

Se även nedan illustration om våra kontakter med Doubletrace.

Sammanfattning av kontakt mellan PwC och Doubletrace