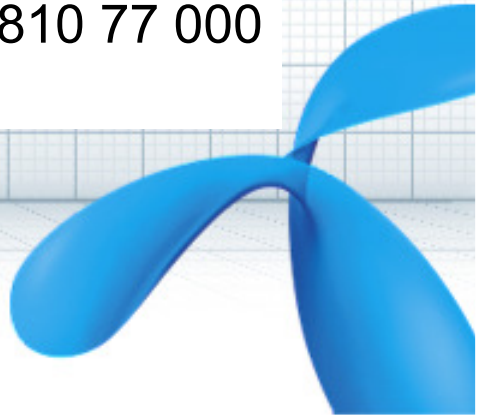
Kontakt

Slå opp og sjekk sikkerhetssenterets blogg som
daglig oppdateres med trusselbilde og aktuelle løsninger.

http://telenorsoc.blogspot.com

Vi stiller gjerne opp i et møte med dere
for å se nærmere på eventuelle løsninger.

Sten Waløen
Internett, Sikkerhet og Datakommunikasjon
Telenor, Business Norway
Tlf.: + 47 47 900 700, Faks +47 947 60 551, Tlf +47 810 77 000
sten.waloen@telenor.com



Telenor Security Operation Centre (TSOC)

Leder Frank Stien
Avdelingsleder TSOC
frank.stien@telenor.com

Noen fakta om TSOC

- Oppstart 2000, avdeling i Telenor 2003
- Egen avdeling som leverer sikkerhetstjenester til bedrifter og partnere med og uten tilknytning til Telenor
- > 100 sikkerhetsmedarbeidere i Telenor – spydspiss med 15 medarbeidere i Arendal
- > 7 år med kontinuerlig sikkerhetsovervåking
- Eksperter på analyse av skadelig kode
  - Publiserer utvalgte deler på telenorsoc.blogspot.com
  - Nyhetsbrev
  - Sikkerhetstest
  - Rådgivning m.m




Media-synlighet

– Det er i første rekke virksomheter som har opplevd et angrep før, som ønsker å bruke penger på teknologi som kan redusere risikoen for angrep, sier avdelingsleder Frank Stien ved Telenor Security Operation center (TSOC) i Arendal. Teknisk Ukeblad 22.08.2008

Kostnadene disse innbruddene medfører burde alene vært nok til å skremme virksomheter som ikke satser på sikkerhetstiltak, til å ta affære. Men mange vet ikke engang at de har blitt kompromitert.

- Det holder ikke med vanlige sikkerhetsverktøy som antivirus, spamfilter og brannmur, forteller Frank Stien, som leder Telenors Sikkerhetssenter, til Finansavisen.

Han mener skadelig kode kan ligge som en tikkende bombe i systemene. Det kan ta lang tid før kriminelle ser sitt snitt til å tjene penger på å tappe virksomheten for id-er eller annen fortrolig informasjon.

Digi.no 29.september 2008

Frank Stien, leder ved Telenor Sikkerhetssenter.

– Alle kan rammes av datakriminalitet. Over halvparten av sensorene Telenor har plassert ut hos kundene har avdekket alvorlige hendelser. Koden kan komme inn i en datamaskin som ble brukt i et eksternt trådløst nett. Det kan vært nok til at kriminelle tar full kontroll over bedriftens datamaskiner når den infiserte maskinen knyttes til bedriftens datanett. Skadelige koder spres også via kjente nettsteder, sier sikkerhetsanalytiker Gunnar Ugland ved Telenor Sikkerhetsenter til Aftenbladet.no. Aftenbladet 22.10.2008

– Du kan surfe på kommunens hjemmeside uten å oppdage en liten tagg. Denne taggen sender deg til en side i Kina, som utløser flere titall angrep mot PC-en din. Resultatet kan være at det lages en bakdør til PC-en, som gjør at man får kontroll over PC-en, sier avdelingsleder Frank Stien i Telenor Security Operation Centre (TSOC). Nrk.no 28.08.2008

Forstår ikke alvoret

I fjor sommer meldte Telenor Security Operations Centre om et massivt hackerangrep mot norske nettsteder. I løpet av en måned ble **over 300 norske nettsteder hacket.**

Det kom blant annet frem at **80 offentlige nettsteder** i Norge var blitt infisert.

Ifølge Telenor Security Operations Center (TSOC) er det ikke er snakk om virus, men om kidnapping av computere. Det vil si at hackere tar kontroll over PC-ene og bruker dem til å angripe andre datamaskiner.

Selv ikke IT-bransjen selv har forstått alvoret, hevder leder for TSOC, Frank Stien.

Store utfordringer

– I land som Kina og Russland kan de it-kriminelle tjene ti ganger så mye som en gjennomsnittlig ingeniørlønn. Dette gir store utfordringer, sier Fra avdelingsleder for TSOC.

I sitt arbeid bruker TSOC en nettverkssensor som genererer spesifikke ra Denne sensoren knyttes gjerne til bedriftens brannmur. Filer sjekkes gru slipper gjennom, og det er hele 13 ulike antivirus-løsninger som er i drift. Alle sensorer inneholder en web-tjener som er tilgjengelig for autorisert personell hos bedriften.

Snartur til Kina.

Fra 1. juni til 26. juni har Telenor Security Operation Centre (TSOC) oppdaget om lag 80 offentlige nettsider som er infisert av datahackere. Økningen er eksplosiv, og vekker bekymring. Aftenposten 30.08.2009

Sårbarheten er toppoppslaget i dagens nyhetsbrev fra Telenor Sikkerhetssenter. IT-sikkerhetsselskapet Secunia klassifiserer sårbarheten som «ekstremt kritisk», altså høyeste farenivå, og Sans Institute har økt trusselnivået til gult i 24 timer.

Digi.no 14.07.09

VG Nett ▸ Teknologi ▸ Artikkel

MSN-trojaneren er farlig

Av Leif Kirknes (Computerworld) og Ole Petter Baugerød Stokke (Computerworld) 13.09.2008 kl. 09:00 Kilde: VG NETT

Trojaneren som ble spredt ut til tusenvis av nordmenn via msn.no er mye farligere enn antatt. Sjekk om du er smittet.

Sikkerhetsarbeid generelt:

- Det finnes ingen ”silver bullet”
- IT-Sikkerhet er kontinuerlig, hardt arbeid
  - Kombinasjon av holdninger, kunnskap og teknologi
- Ingen enkeltløsning håndterer alle sikkerhetsutfordringer
- Sikkerhet er et ledelsesansvar

Franks teori:

God Sikkerhet =

(sunne holdninger x forstått ansvar x riktig teknologi x
oppdatert kunnskap x høy kompetanse) x 24x365

Hvor ille er det?

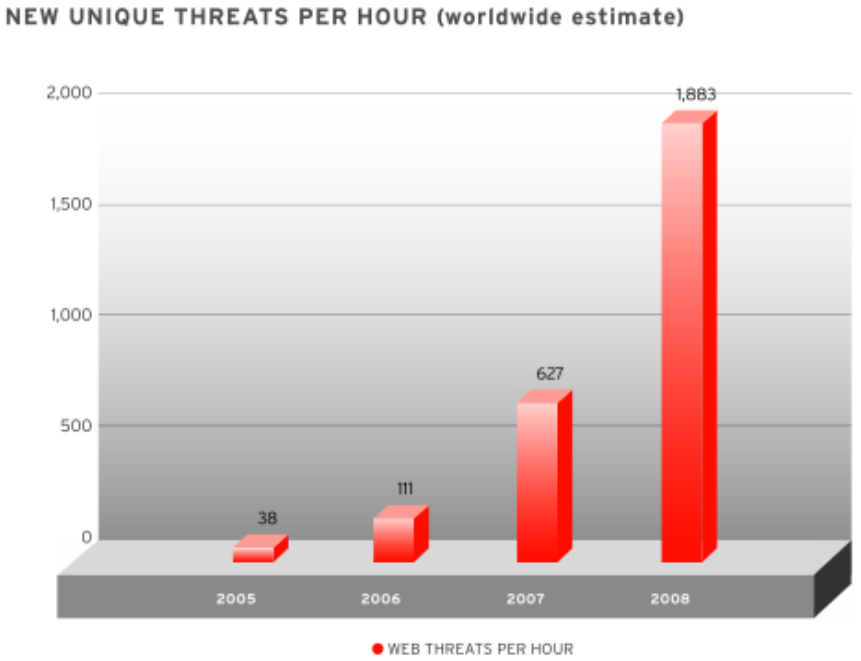


Figure 2: Steady increase in web threats

Ref: Trend Micro (blog.trendmicro.com)

14.10.2009:

- Microsoft sender ut 13 patcher til operativsystemene. Mange kritiske!
- Adobe sender ut oppdatering til Acrobat og reader som fikser 29 (!) svakheter. Mange kritiske!

#	Affected	Contra Indications	Known Exploits	Microsoft rating	ISC rating(*) clients	ISC rating(*) servers
MS09-050	Vulnerabilities in SMBv2 Could Allow Remote Code Execution (Vista and Windows Server 2008 SP2 only)					
	SMBv2 CVE-2009-2526 CVE-2009-2532 CVE-2009-3103	KB 975517 first mentioned in KB 975497	CVE-2009-3103 is publicly known! see our diary here.	Severity:Critical Exploitability:3,1,1	Critical	Critical
MS09-051	Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution					
	Windows Media Runtime CVE-2009-0555 CVE-2009-2525	KB 975682	CVE-2009-0555 known publically	Severity:Critical Exploitability:1,2	Critical	Important
	r Could Allow Remote Code Execution					
			own its.	Severity:Critical Exploitability:1	Critical	Critical
	ernet Information Services Could Allow Remote Code Execution					
			its Known oth rabilities!	Severity:Important Exploitability:3,1	Important	Critical
	rnet Explorer					
			its known			

Telenor Sikkerhetssenter - Daglig nyhetsbrev 2009.10.14

Kommentar til dagens nyhetsbrev:

Microsoft har sluppet sikkerhetsoppdateringene for oktober. Denne gangen er det hele 13 patcher som er ute, hvorav mange er å anse som kritiske.

I tillegg har Adobe også kommet med en stor oppdatering til Acrobat og Reader som tetter ikke mindre enn 29 svakheter.

Adobe Reader and Acrobat Multiple Code Execution Vulnerabilities

Type	Alvorlighetsgrad	Kategori	Dato	ID
Ekstern kodeeksekvering	Kritisk	Svakhet	2009-10-14 06:25:39	6810

Analytikers kommentar

Adobe har i løpet av natten sluppet en oppdatering for Reader og Acrobat som tetter hele 29 svakheter, bl.a. sikkerhetshullene vi meldte fra om i forrige uke. Se anbefaling for link til patch og referanse for mer informasjon.

Sårbare systemer	Anbefaling
Adobe Reader versjon 9.1.3 og tidligere (Windows, Macintosh, and UNIX) Adobe Reader versjon 8.1.6 og tidligere (Windows, Macintosh, and UNIX) Adobe Reader versjon 7.1.3 og tidligere (Windows and Macintosh) Adobe Acrobat versjon 9.1.3 og tidligere (Windows, Macintosh, and UNIX) Adobe Acrobat versjon 8.1.6 og tidligere (Windows, Macintosh, and UNIX) Adobe Acrobat versjon 7.1.3 og tidligere (Windows and Macintosh)	Oppgrader til Adobe Acrobat og Reader med versjonsnummer 9.2, 8.1.7, eller 7.1.4: http://www.adobe.com/go/gntray_prod_acrobat_family_home

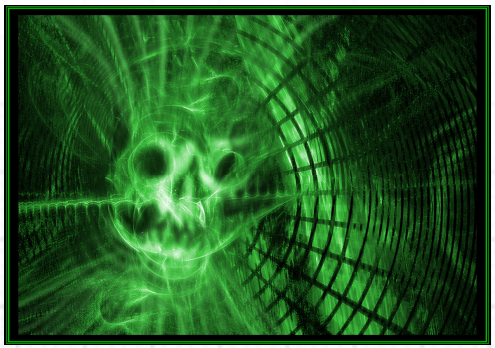
Referanser

http://www.adobe.com/support/security/bulletins/apsb09-15.html

Ref: SANS

Oppsummering – hva ser vi hos TSOC?

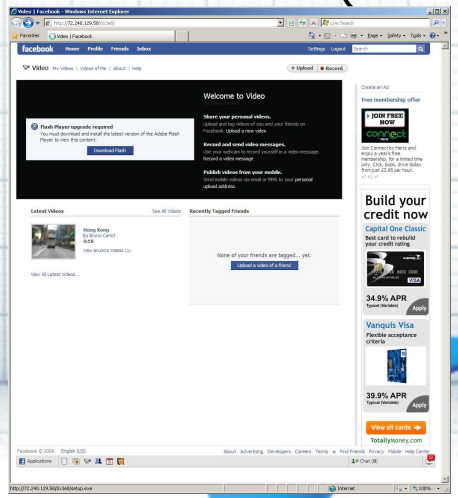
Drive-by (javascipt)



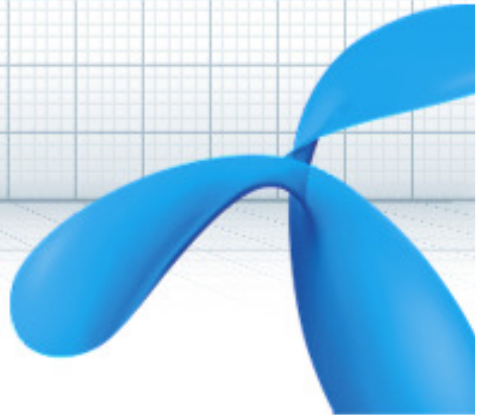
Ondsinnet banner reklame

Falske antivirus

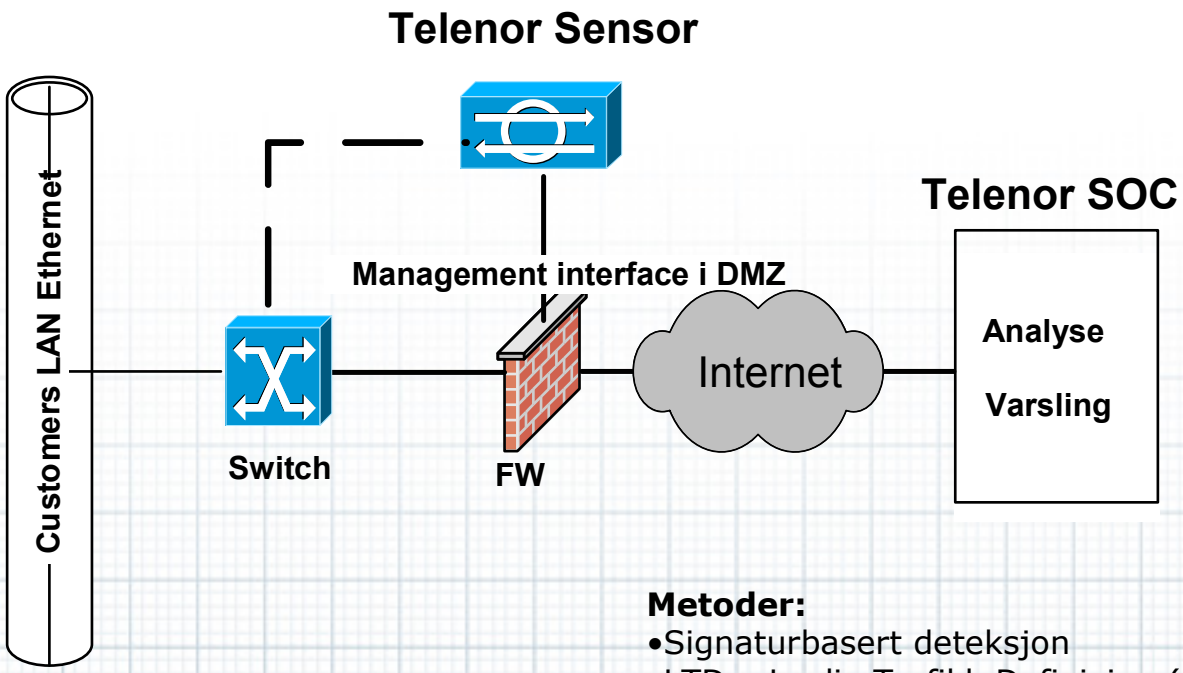
Falske oppdateringer i sosiale nettverk (Koobface)



Så litt om tjenesten vår..



Network Security Monitoring (evt. IDS)

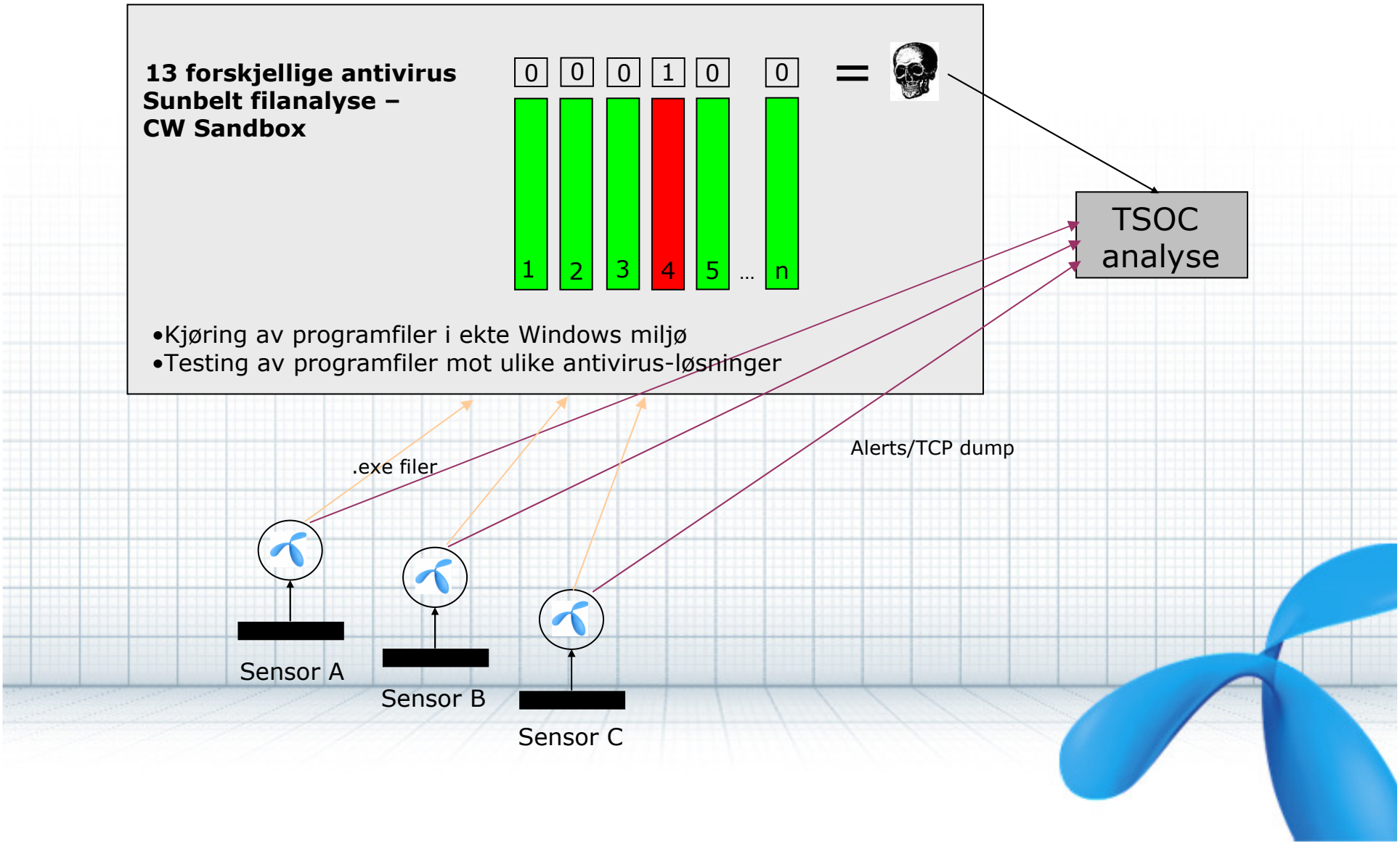


Metoder:

- Signaturbasert deteksjon
- LTD – Lovlig Trafikk Definisjon (SYN ACK)
- Black-listing av fiendtlige adresser
- Statistiske metoder
- Kundespesifikke mønster
- SANDMAN (sandbox analyse)

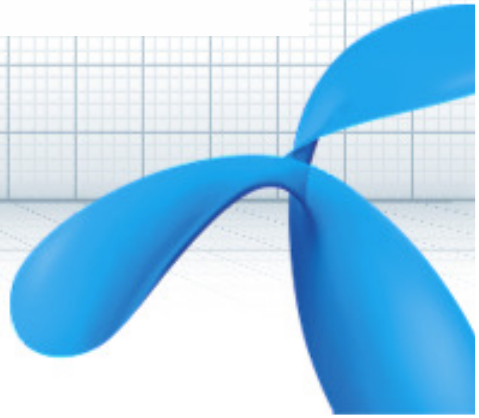
med mer….

Telenors Network Security Monitoring

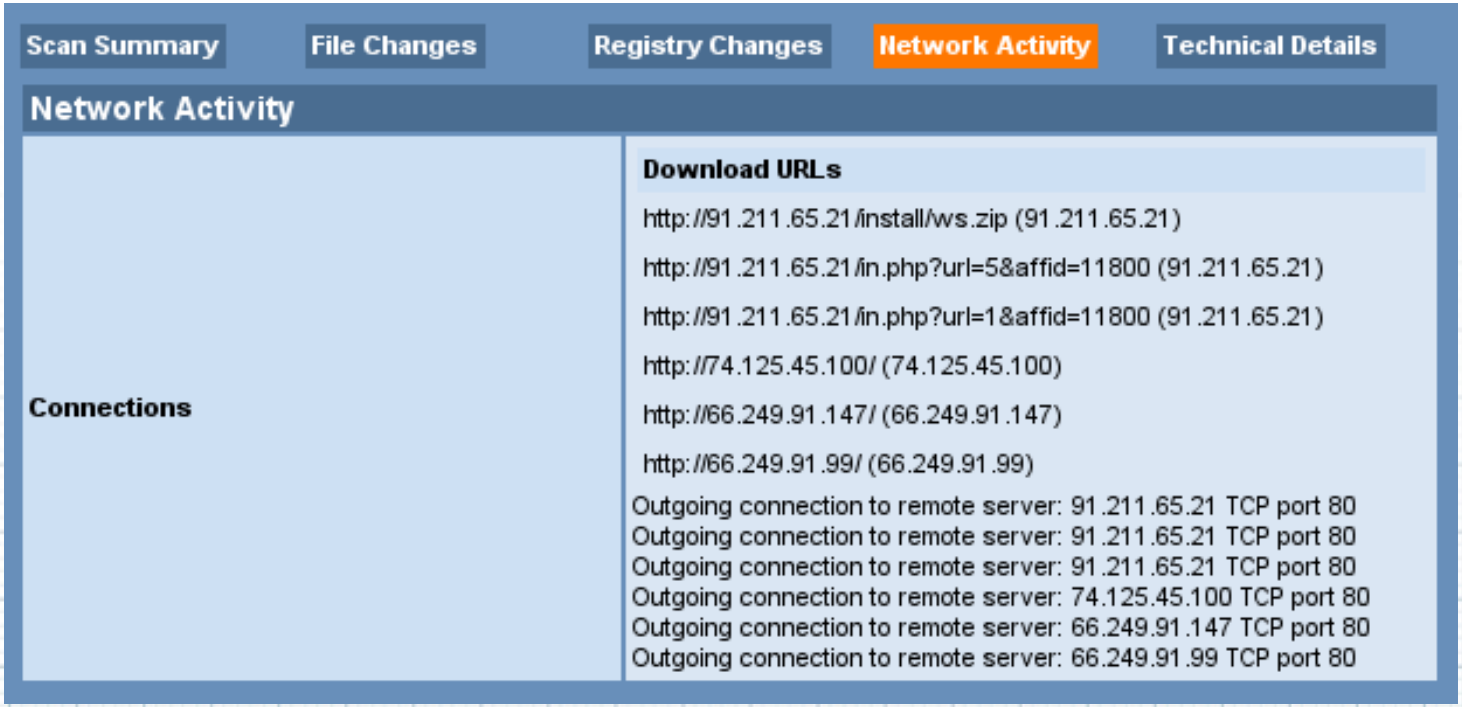


Analyserer alle mistenkelige filer med 11 antivirus

```
                    *** SANDMAN ANTI-VIRUS RESULTS ***

Filename: [redacted]

Antivirus  Version    Last sig. update    Scanning timestamp  Result
-------------------------------------------------------------------
   fsecure 7.00.171   2009-01-06 00:00:00 2009-01-06 21:06:51 OK
      clam UNKNOWN    UNKNOWN             2009-01-06 21:06:30 OK
   antivir 7.1.1.69   2009-01-05 00:00:00 2009-01-06 21:06:30 OK
    norman 5.99.02    UNKNOWN             2009-01-06 21:06:54 OK
     fprot 6.2.1.4201 2009-01-06 18:36:00 2009-01-06 21:06:51 OK
     avast UNKNOWN    2009-01-06 00:00:00 2009-01-06 21:06:55 OK
       nod 3.0.657.0  2009-01-06 00:00:00 2009-01-06 21:06:34 OK
       kav UNKNOWN    UNKNOWN             2009-01-06 21:06:31 OK
  symantec 4.3.2.10   2009-01-06 00:00:00 2009-01-06 21:06:28 OK
     trend 8.700-1004 2008-12-17 00:00:00 2009-01-06 21:06:43 PAK_Generic.001
       avg 8.0.145    2009-01-06 00:00:00 2009-01-06 21:06:34 Trojan horse Downloader.Generic8.MLN

                    ****************************************
```



Analyse av potensielt skadelig kode



TSOCs blog - **http://telenorsoc.blogspot.com**

www.telenorsoc.blogspot.com/

telenor **TSOC-blogg**
- en sikkerhetsblogg

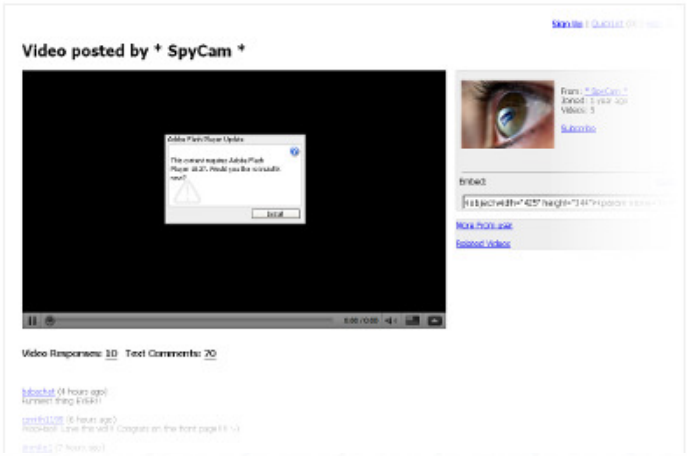
Vi gjør oppmerksom på at informasjonen gitt i denne bloggen er ferskvare og således kan inneholde feil. Aksjoner som gjøres på grunnlag av denne er på eget ansvar. Telenor tar ikke ansvar for innhold gitt i eksterne lenker.

22. september 2009

Koobface benytter exploits

I tillegg til de vanlige falske Flash-oppdateringene, har vi nå observert at bakmennene bak Koobface benytter exploits for å spre denne ormen.

De ferskeste linkene til Koobface har også en oppdatert side som skal lure brukere til å installere en falsk oppdatering av Flash. Tittelen på de nye sidene er "Video posted by * SpyCam *", og ser slik ut:



Om Telenor SOC

Telenor SOC (TSOC) er en avdeling i Telenor som driver en 24/7-tjeneste for sikkerhetsovervåking av kunders nettverk.

Våre analytikere gjør kontinuerlig analyse av uønsket aktivitet på internett, og vi ønsker med denne bloggen å bidra med teknisk informasjon som kan være til nytte for andre i sikkerhetsmiljøet.

Kontaktinformasjon

Epost: tsoc (a) telenor.net

Lenker

- Telenor Network Security Monitoring
- Telenor Bedrift Sikkerhet
- ISC Diary

Creative Commons

t4kk f0r m3g.