

ATTACK ORIGINS

#	Country
715	China
584	United States
265	Spain
92	Canada
87	Hong Kong
73	Russia
73	France
64	Mil/Gov
54	Netherlands
42	Italy

ATTACK TARGETS

#	Country
1802	United States
104	Hong Kong
63	Thailand
52	Bulgaria
39	Canada
39	United Kingdom
39	France
39	Australia
33	Norway
32	Liechtenstein

ATTACKS

Timestamp	Attacker			Target		Type
	Organization	Location	IP	Location	Service	
2014-06-25 14:11:43.16	Embarq Corporation	Lady Lake, United States	71.51.87.47	San Rafael, United States	sco-inetmgr	615
2014-06-25 14:11:44.01	LaFrance Internet Services	Rancho Cordova, United States	74.82.47.37	San Leandro, United States	gold	17
2014-06-25 14:11:44.89	Unitedlayer	Livermore, United States	209.237.228.186	Hays, United States	NetController, ntp	123
2014-06-25 14:11:45.76	COLOMBIA	Montelbano, Colombia	186.113.12.135	unknown, Hong Kong	unknown	11258
2014-06-25 14:11:46.63	Gigahost Limited	unknown, Hong Kong	117.18.69.185	unknown, Hong Kong	netbios-dgm	138
2014-06-25 14:11:46.64	Gigahost Limited	unknown, Hong Kong	117.18.69.183	unknown, Hong Kong	netbios-dgm	138
2014-06-25 14:11:46.65	Gigahost Limited	unknown, Hong Kong	117.18.70.148	unknown, Hong Kong	netbios-dgm	138
2014-06-25 14:11:47.48	Gigahost Limited	unknown, Hong Kong	117.18.70.167	unknown, Hong Kong	netbios-dgm	138

ATTACK TYPES

#	Service	Port
363	telnet	23
167	ssh	22
143	unknown	29991
136	microsoft-ds	445
107	domain	53
96	https	443
91	CrazyNet	17500
90	netbios-dgm	138



011001001101010001100101000100101010100011

Nationalt Cyber Crime Center

Hvordan bekæmper man cyberkriminalitet anno 2015

Kriminalitetsudviklingen i Danmark

- Kriminaliteten falder..!
- Cyberkriminaliteten stiger
 - Økonomisk vinding
 - Traditionel bandekriminalitet
 - Mindre straffe
 - Nemmere at gemme sig
 - Nemt at komplicere juridisk (int)
 - Mindre fysisk fare for en selv



UDVIKLING I IT-SAGER HOS POLITIET

	2009	2010	2011	2012	2013	2014
Hacking	39	146	42	40	95	167
Alvorlig hacking	4	0	1	2	0	11
Databedrageri	694	1340	559	1366	2421	4583
Tyveri fra pengeautomat	2864	2875	4009	3375	3748	3314

Kilde: Rigspolitiet

Note: Det skal understreges, at dette ikke er det fulde billede, da en række økonomiske sager reelt er it-kriminalitet, og derfor ikke figurerer i ovenstående skema. Politiet er i gang med en fintælling af it-sager, så der i løbet af 2015 kommer et mere retvisende billede af it-kriminaliteten i Danmark.

Hvad skal der til?

Kompetence

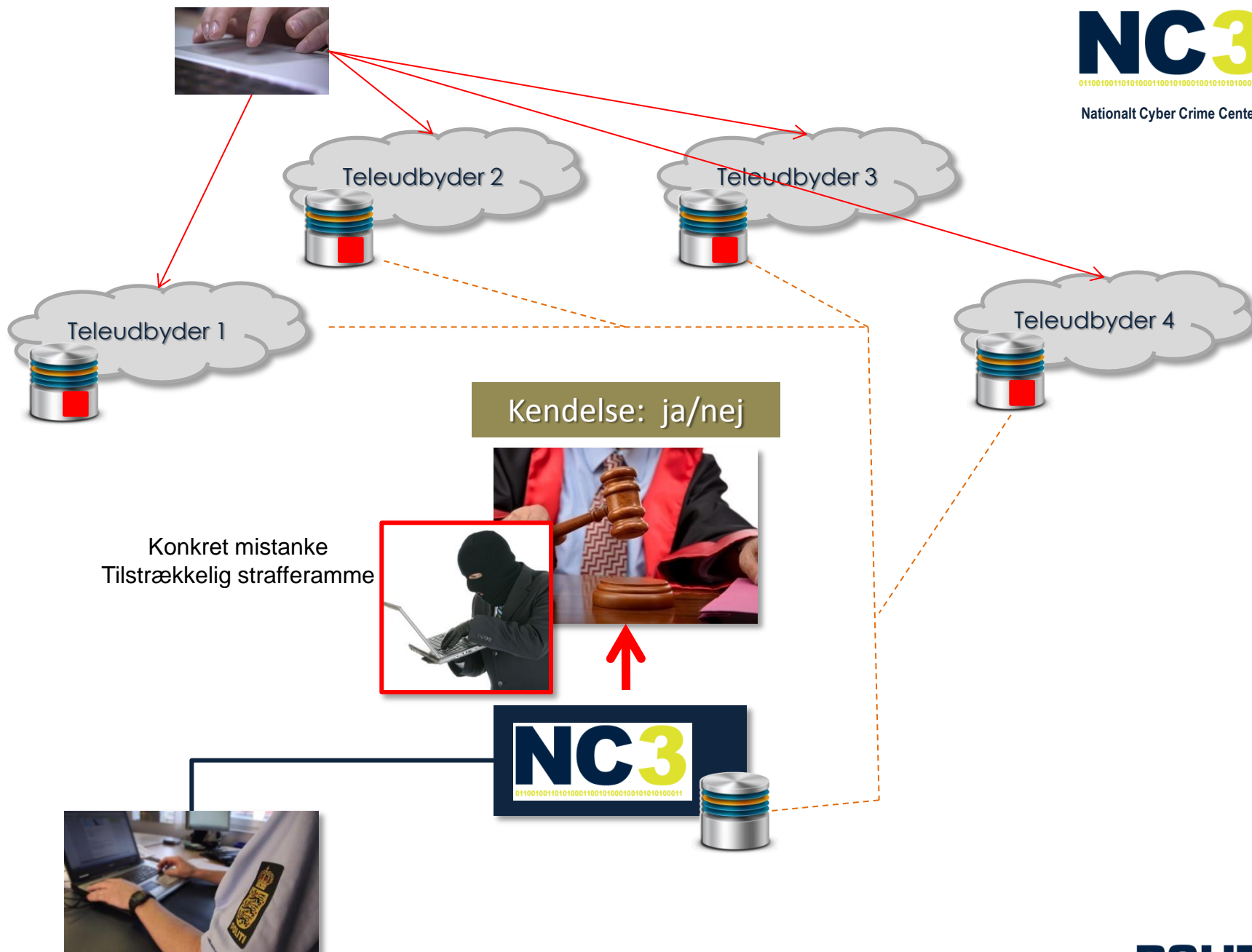
Kapacitet

Teknologi

Processer

- Mange digitale aftryk hver dag
- Skift mellem flere udbydere
- Skift mellem mange services





Udfordringer

- International grænseoverskridende kriminalitetsform
- Konstant metodemæssig bevægelse – i vækst – kræver høj grad af agilitet
- Anonyme tjenester (Tor) og skjult internet (Silk Road / dark web)
- Virtuel valuta (bitcoin) der ikke kan spores
- Skift fra IPv4 til IPv6 -> (4.000.000.000 (4 mia) til
340.000.000.000.000.000.000.000.000.000.000.000.000.000..)
- Flere får smartphones og bærbare enheder, der kan hacke og hackes
- Cloud tjenester (forskellige nationale lovgivninger)
- Langsom reaktion hos andre myndigheder
- Forskellige nationale prioriteringer

CaaS – Crime as a Service

Table 1. Prices for zero-day vulnerabilities.

Adobe Reader	\$5,000–\$30,000
Mac OS X	\$20,000–\$50,000
Android	\$30,000–\$60,000
Flash or Java Browser Plug-ins	\$40,000–\$100,000
Microsoft Word	\$50,000–\$100,000
Windows	\$60,000–\$120,000
Firefox or Safari	\$60,000–\$150,000
Chrome or Internet Explorer	\$80,000–\$200,000
iOS	\$100,000–\$250,000



France Email Database 1 million Available **PRICE LOWERED!**
France Email Database 1 million
\$495.49
[Add to cart](#)
[View](#)



USA DOCTOR EMAIL DATABASE
USA Doctor email Database (0.7 Million)
PRICE LOWERED!
\$114.34 tax incl.
~~\$127.65 tax incl.~~
(price reduced by 10 %)
Quantity :
Availability: 999 items in stock
[Add to cart](#)
[Add to my wishlist](#)
PayPal
Click here to pay

Sager

- Seksuelt misbrug af børn
- Narkotikahandel via Silk Road (Tor og Bitcoin)
- Scareware/Ransomware/cryptolocker
- DDoS som afpresning / eller som hacktivism
- Hackning af kundedatabaser (Password/UserID/kreditkort)
- Hackning af dansk politi's mainframe system (CSC sagen)
- Hacktivism generelt (bl.a. rettet mod vores politikere)
- Svindel i alverdens varianter
- Digital støtte i alle typer sager – herunder i rettighedssager

Rettighedsområdet

- Tæt og udbredt samarbejde mellem SØIK, NC3 og politikredsene
- Uddannelsesstøtte (bl.a. it-forensics, og vedr. digital valuta m.m.)
- Koordination både nationalt og internationalt -> efterforskningsoplæg
- Ransagningsstøtte i snit en gang om ugen, og i en række forskellige typer af sager, herunder cardsharing sager (2014 = 12 sager)
- Indsatsen intensiveres yderligere i 2015
- Udlæsninger af mobil & tablets udlæses
- HTC vil i 2015 forøge fokus på online/osint området, og vil derigennem proaktivt udfærdige efterforskningsoplæg herunder inden for IPR området.
- Innovation, idet omfang SØIK selv melder noget ind

Kontakt



Kim Aarenstrup
centerchef

Rigspolitiet

Politiområdet - NC3
Nationalt Cyber Crime Centre
Polititorvet 14
1780 København V
E-mail: kaa006@politi.dk