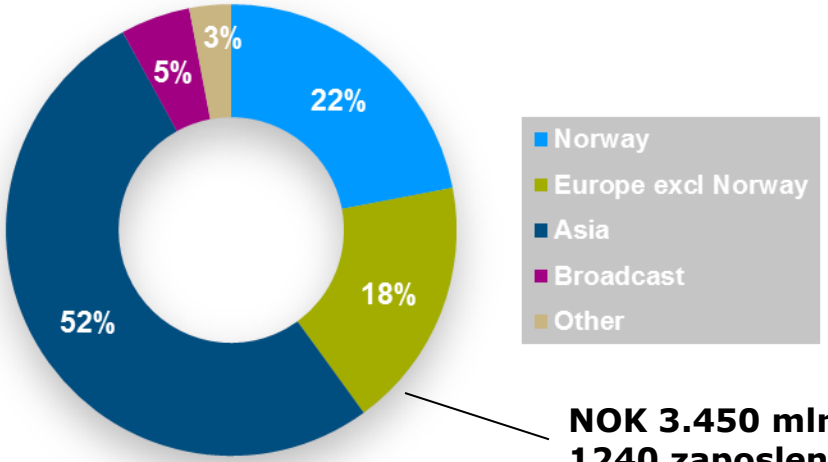
Sajber bezbednost i komercijalni sektor

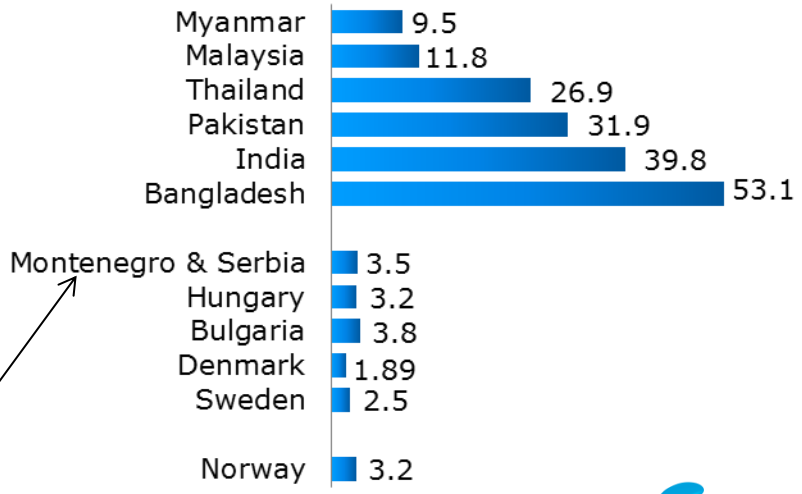
Javno slušanje u Skupštini Republike Srbije
10. septembar 2015.

Telenor groupa

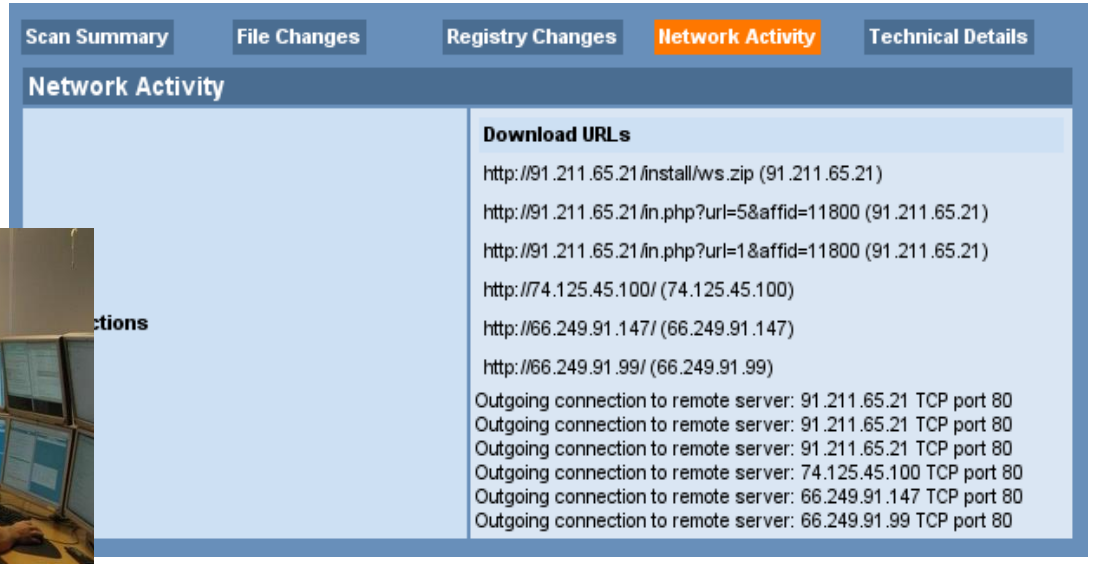
- Mobilne operacije u 13 zemalja: Skandinavija, Evropa i Azija
- 189 mil. mobilnih korisnika
- 43 % glasačkog udela (33% ekonomskog) u ruskom VimpelCom Ltd. sa 218 mill. mobilnih korisnika na 14 tržišta
- Prihod u 2014: 107 mlrd NOK
- Oko 33.000 zaposlenih

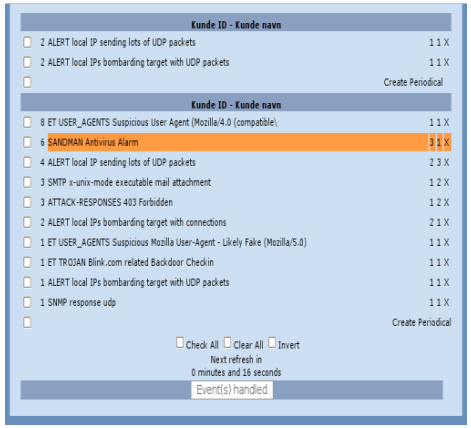


NOK 3.450 mlrd
1240 zaposlenih



TSOC





- **TSOC** alarm
- IT operacije izoluju incident (PC, cdr)
- Formiran CMT
- Identifikovan izvor infekcije
- Ciljani napad!

NSM NorCERT

FORSVARET Cyberforsvaret

Naredni dani

- Forenzičke analize
- Korisnici – procena rizika
- Prijava KRIPOS, informacija medijima
- Analiza štete

KRIPOS

telenor

N
norman
May 2013

OPERATION HANGOVER

Unveiling an Indian Cyberattack Infrastructure

Snorre Fagerland, Morten Kråkvik, and Jonathan Camp
Norman Shark AS

Ned Moran
Shadowserver Foundation

Part of a PDF decoy from one of the malicious installers (md5 [illegible]).

TechCentral.ie

Telenor cyberattacks from mystery Indian hacking group

Attacks carried out on global scale, said Norman Shark

Tech4Biz | 21 May 2013 : The large-scale cyberattacks that hit Norway's state telecoms firm Telenor in March didn't originate from China as many assumed but from a previously unknown Indian cybercrime group, an analysis by Norman Shark has found.

Significantly, the incident was not an isolated assault and appears to be part of a much larger industrial espionage campaign targeting multiple firms across the globe, the company said.

See also...

Mozilla advises Firefox users to disable McAfee plugin
6982

Symantec confirms Adobe Reader exploits targeted defence companies
5114

Some positive trends in a challenging

Is India a new front line for the spread of large-scale cybercrime?

According to Operation Hangover (co-authored with a Shadowserver Foundation researcher), the mysterious group they now believe was the source of this attack has been especially active in 2012 and so far in 2013 having been in existence for as long as four years.

The Telenor attacks were assumed by some to have come from China simply because large-scale APTs are now firmly associated with that country. It appears they might have underestimated the capabilities of non-Chinese hacking groups doing the job on a jobbing basis.

ComputerWeekly.com

Home > Topics > IT security > Privacy and data protection > Norway's Telenor hit by cyber espionage campaign

CYBER SECURITY

Norway's Telenor hit by cyber espionage campaign

Warwick Ashford
Tuesday 19 March 2013 09:42

Share 1 +1 1 Tweet 17

Norwegian telecoms provider Telenor has been hit by a major cyber espionage campaign, carried out by attackers who stole files and emails from unnamed executives.

The company has reported the matter to the police and the national CERT, but said the breach had been detected quickly and steps had been taken to prevent future incidents, according to local reports.

Telenor has also notified Norway's national security authority and the cyber defence unit.

The attackers used phishing emails that appeared to come from trusted contacts to trick executives into downloading malware designed to steal login credentials, emails, and personal and commercial data.

the security ledger

BUSINESS ▾ | CONSUMER ▾ | GOVERNMENT ▾ | THREATS ▾ | HACKS &

You are here: Home » Business » ISP Telenor: Execs Laptops Emptied in Cyber Spy Operation

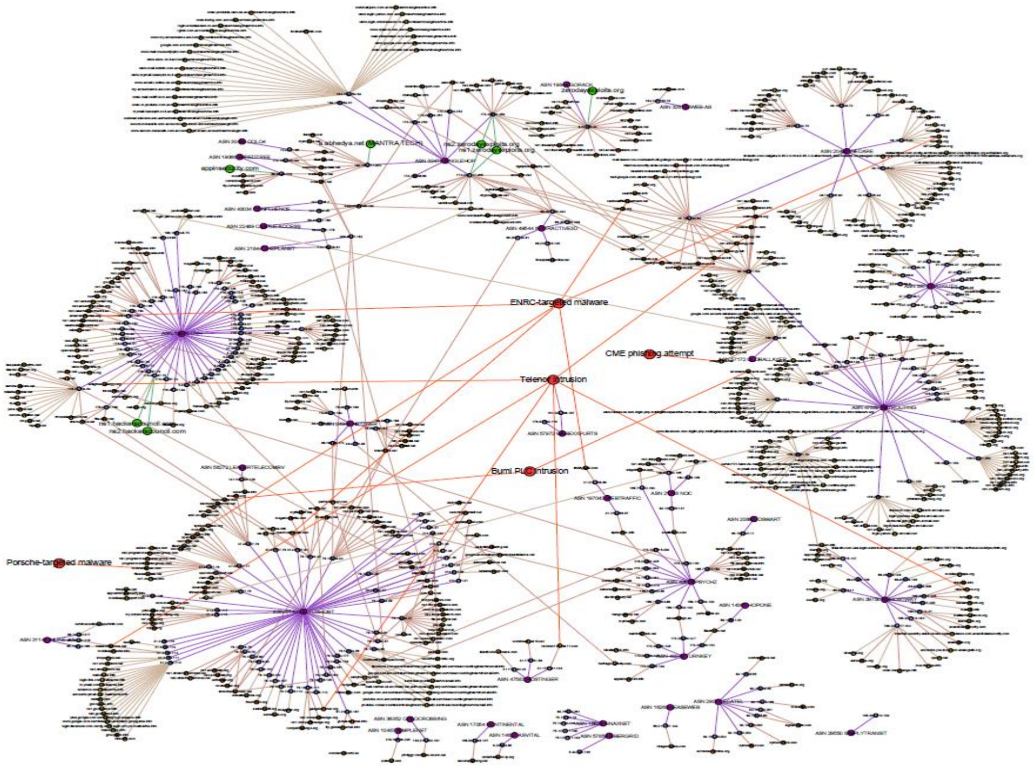
ISP Telenor: Execs Laptops Emptied in Cyber Spy Operation

MARCH 18, 2013 14:37 0 COMMENTS

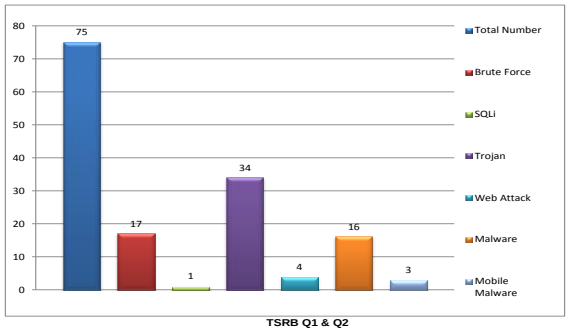
The Norwegian telecommunications firm Telenor told authorities in that country that a sophisticated cyber spying operation compromised the computers of leading executives and "emptied" them of sensitive information, including e-mail messages, computer files and passwords, according to a report Sunday by Aftenposten.

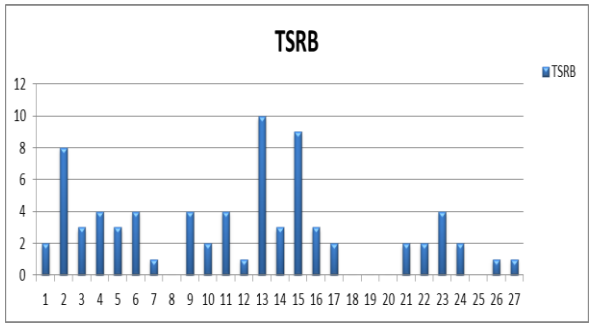
Norwegian ISP Telenor said that its executives were hacked in a case of cyber espionage.

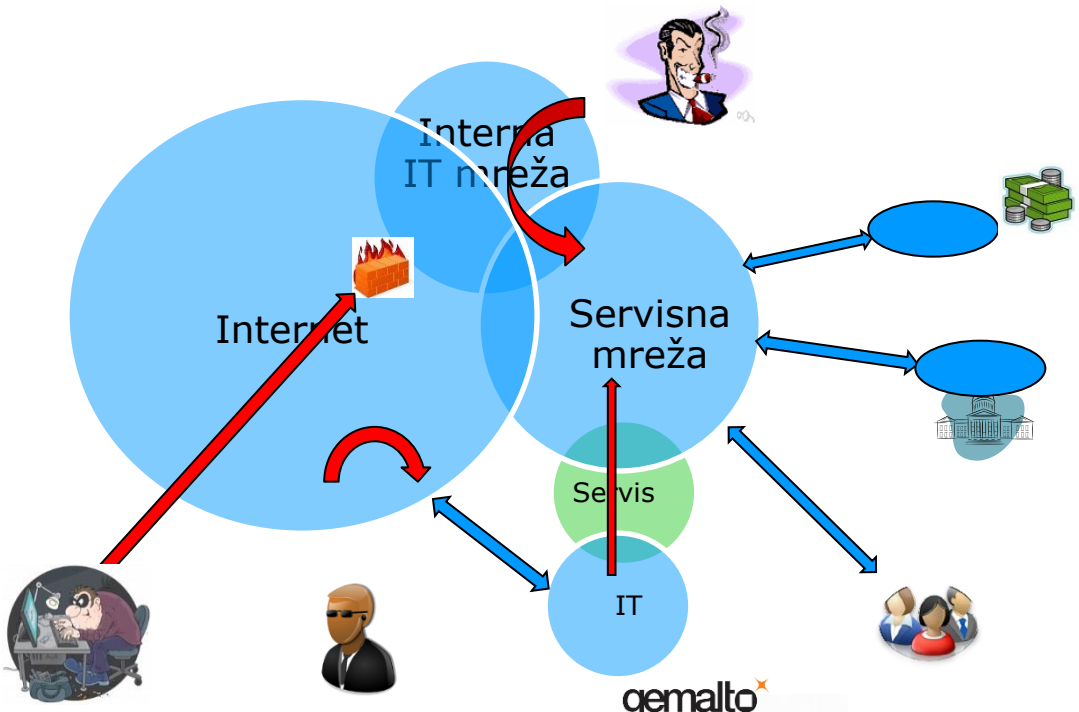
Several executives of Telenor were the subjects of "extensive, organized industrial espionage," the report said, quoting Telenor Norway's director, Rune Dyrlie. The company has reported the incident to Nasjonal sikkerhetsmyndighet – or NSM - Norway's national security authority *as well as* Nor-CERT, Norway's Computer Emergency Readiness Team and the cyber defense unit Cyberforsvaret.



telenor

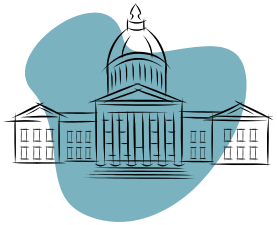

Total Number
Brute Force
SQLi
Trojan
Web Attack
Malware
Mobile Malware
75
17
1
34
4
16
3
TSRB Q1 & Q2


TSRB
TSRB


Interna IT mreža
Internet
Servisna mreža
Servis
IT
gemalto
security to be free
BELGACOM


CNE access to core mobile networks
CNE access to core mobile networks
Billing servers to suppress SMS billing
Authentication servers to obtain K's, Ki's and OTA keys
Sales staff machines for customer information and network engineers machines for network maps
GEMALTO – successfully implanted several machines and believe we have their entire network – TDSD are working the data

Ko je odgovoran za sajber bezbednost?



?

Korisnici

Komponente

Operativni sistemi

Uređaji

IKT usluge sa dodatnom vrednošću OTT

Operator IKT

Aplikacije

Marketi aplikacija

Proizvođači Integratori

Partneri Usluge

Fizička lica

Poslovni

Državni organi

SCADA IoT

Izazovi sajber bezbednosti

Ekonomski

- Vlasništvo i očekivanja akcionara
- Troškovi, finansiranje i motivacija
- Tržišna utakmica (TTM), bezbednost nije prioritet

Tehnološki

- Digitalna ekonomija,novi biznis modeli, razvoj tehnologije, konvergencija domena
- Napadači (kapaciteti, brojnost, motivacija, prednost)

Politički

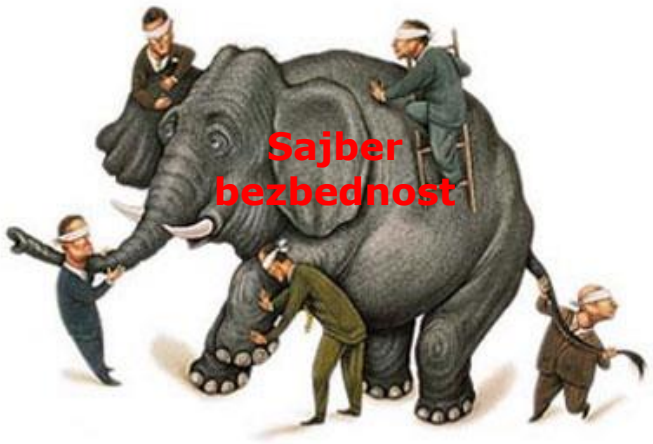
- Balans ekonomski razvoj – bezbednost; zaštita – deljenje informacija
- Različiti akteri i interesi
- Multi partnerski rad na različitim pitanjima
- Poverenje
- Percepcija (pojedinci i javnost)

Ljudski faktor

- Insajder (personal operatora, partneri, zla namera, nemar)
- Korisnici

telenor

Kako dalje?



- **Osvešćenost**
  - Kultura sajber bezbednosti
  - Kultura privatnosti
- **Uspostavljanje poverenja među akterima**
  - Formalizacija saradnje
  - Slobodna komunikacija
- Odgovarajući **skup standarda zaštite** razvijen u saradnji sa privatnim sektorom
- **Koncentracija resursa**
- **Javno-privatno partnerstvo**
  - Formulisanje politika i zakona
  - Operativne mere zaštite
  - Deljenje informacija
  - Komunikacija sa korisnicima
  - Obuka
  - Incidentne situacije
- **Nivoi saradnje**:
  - Odbrana i zaštita kritične infrastrukture
  - Zaštita komercijalnih mreža i usluga
  - Civilno društvo

telenor

Hvala na pažnji

?

Milan Nikolić
Direktor korporativne bezbednosti
Lokalni oficir za zaštitu privatnosti

Telenor
milan.nikolic@telenor.rs