GJØVIK UNIVERSITY COLLEGE

Security planning and Incident Management

Marie Moe, NSM/HiG

Gjøvik 13.01.14

AGENDA

- About me
- Threats to Information Security – Why we need Security Incident Management and Planning
- About this course
- Literature
- Project work
- Important dates

ABOUT ME

- Senior Engineer at NSM NorCERT
- Associate Professor II at HiG (20%)
- MSc in Mathematics
- PhD in Information Security
- GIAC certified Incident Handler

Email: marie.moe@hig.no/
marie.moe@nsm.stat.no
Twitter: @MarieGMoe

FOTO: ROBERT MCPHERSON, Aftenposten

THREATS TO INFORMATION SECURITY

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Deviation in quality of service by service providers	Power and WAN quality-of-service issues service providers
Technical hardware failure or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescense	Antiquated or outdated technologies

M. E. Whitman, "Enemy at the Gates: Threats to Information Security", Communications of the ACM 46 (2003): 91-95. Also see Whitman and Mattord 2007, p. 5.

Let’s look at some examples…

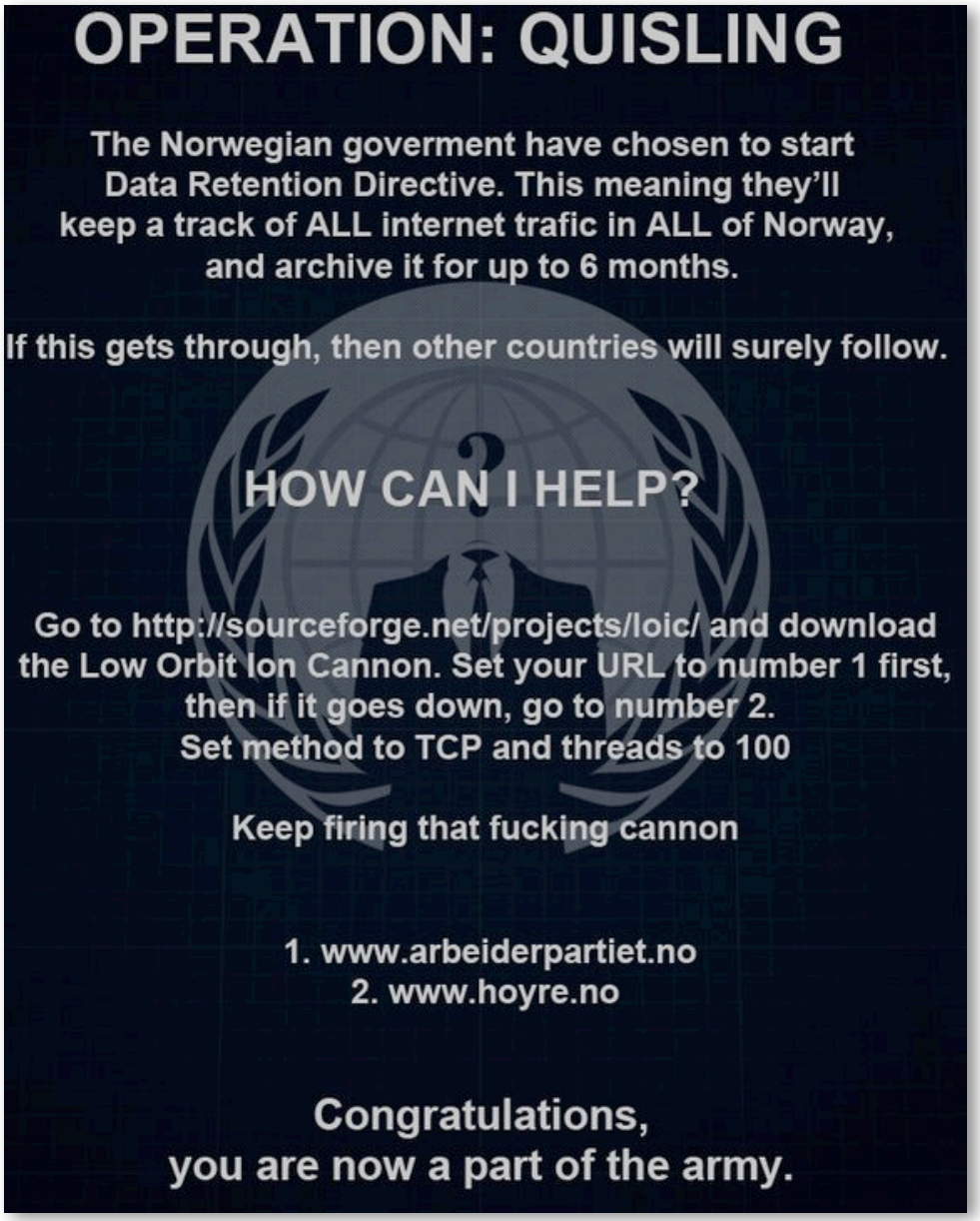
50 Days of Lulz

BY: A GUEST ON JUN 25TH, 2011 | SYNTAX: NONE | SIZE: 4.71 KB | HITS: 441,669 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT


```
. /$$                 /$$            /$$$$$$
.| $$                | $$           /$$__  $$
.| $$       /$$   /$$| $$ /$$$$$$$$| $$  \__/  /$$$$$$   /$$$$$$$
.| $$      | $$  | $$| $$|____ /$$/|  $$$$$$  /$$__  $$ /$$_____/
.| $$      | $$  | $$| $$   /$$$$/  \____  $$| $$$$$$$$| $$
.| $$      | $$  | $$| $$  /$$__/   /$$  \ $$| $$_____/| $$
.| $$$$$$$$|  $$$$$$/| $$ /$$$$$$$$|  $$$$$$/|  $$$$$$|  $$$$$$.$
.|________/ \______/ |__/|________/ \______/  \_______/ \_______/
                          //Laughing at your security since 2011!


.--    .-""-.
.   ) (     )
.  (   )   (
.     /     )
.    (_    _)                    0_,-.__
.      (_  )_                    |_.-._/
.       (    )                   |lulz..\
.        (__)                    |__--_/
.     |''   ``\                  |
.     | [Lulz] \                 |      /b/
.     |         \  ,,,---===?A`\  |  ,==y'
.   ___,,,,,----=""\        |M] \ | ;|\ |>
.           _   _   \   ___,|H,,---==""""bno,
.    o  O  (_) (_)   \ /          _     AWAW/
.                     /         _(+)_  dMM/
.      \@_,,,,,,---=="   \      \\|//  MW/
.--'''''"                        ===  d/
.                                    //   SET SAIL FOR FAIL!
.                                    ,'_____________________________
.   \    \    \     \              ,/~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```



http://imgur.com/r/4chan/BI35Q

SECURITY

Norwegian teens arrested over SOCA DDoS attack

Also accused of pwning online newspaper, financial services group

By John Leyden, 10th May 2012

Norwegian police have charged two teenagers suspected of taking part in denial of service attacks against the UK's Serious Organised Crime Agency and other targets.

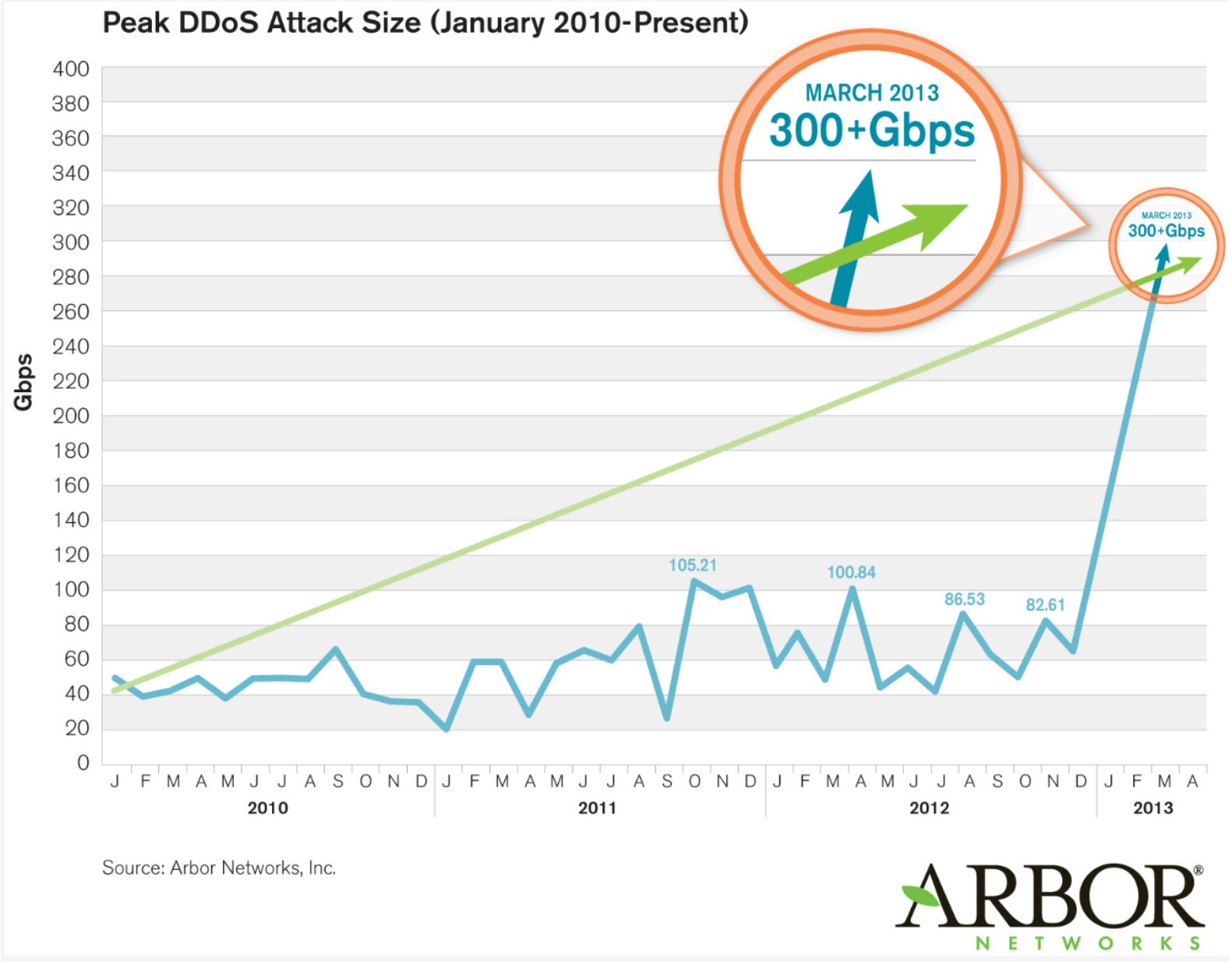
RELATED STORIES

Hackers threaten fresh wave of anti-capitalist web rioting

The unnamed youngsters (aged 18 and 19) are also suspected of attacking the Norwegian financial services group DNB and Germany's *Bild* newspaper, according to Norwegian reports.

"We have arrested the two we think were most important in these attacks, but we still want to talk to more people," Norwegian prosecutor Erik Moestue told the BBC.

http://www.theregister.co.uk/2012/05/10/soca_ddos_arrests/



http://www.arbornetworks.com/corporate/blog/4813-putting-the-spamhouse-ddos-attack-in-perspective

BGPMON

HOME BLOG ABOUT US PRODUCTS AND SERVICES NEWS AND PRESS CLIENT PORTAL

Looking at the spamhaus DDOS from a BGP perspective

Posted by Andree Toonk - March 30, 2013 - BGP instability, Hijack - 1 Comment

It's been a busy week for network engineers world wide, rerouting around broken optical links and of course the 300Gb/s DDOS attack towards Spamhaus and Cloudflare. This DDOS has been classified as the largest DDOS attack ever recorded and has been written about quite a bit in mainstream media.

There's been a bit of discussion about how much this DDOS actually slowed down the Internet globally. Fact is that the Internet didn't come to a halt but the large amount of new traffic that had to be handled by some of the carriers did result in congestion and significant packet loss by some of the Tier1 carriers last weekend. In this blog post we'll look at this event from the routing perspective, what effects did this have on the Internet Exchanges and we'll also look at some BGP hijacks related to this attack.

https://www.bgpmon.net/looking-at-the-spamhouse-ddos-from-a-bgp-perspective/

DoS attacks that took down big game sites abused Web's time-sync protocol

Never-before-seen technique abused the Network Time Protocol to worsen effects.

by **Dan Goodin** - Jan 9 2014, 12:47am CET

BLACK HAT PC GAMING 69

69 percent of all DDoS attack traffic by bit volume in the first week of January was the result of NTP reflection.

Black Lotus

http://arstechnica.com/security/2014/01/dos-attacks-that-took-down-big-game-sites-abused-webs-time-synch-protocol/

Microsoft Official Blog and Twitter account hacked by Syrian Electronic Army

by **Wang Wei** on Saturday, January 11, 2014

http://thehackernews.com/2014/01/microsoft-official-blog-and-twitter.html

http://thehackernews.com/2014/01/microsoft-official-blog-and-twitter.html

http://www.techienews.co.uk/974686/sea-hijacks-official-xbox-support-twitter-account/

Yikes! Target's data breach now could affect 110M people

The retailer now says that information taken in December's security lapse includes names, phone numbers, and postal and e-mail addresses, and could affect up to one-third of the US population.

by Don Reisinger | January 10, 2014 11:48 AM PST

639 152 25 +1 190 More + Comments 112

(Credit: Target)

Target's data breach is much broader than once believed

The nationwide retailer on Friday announced t

c|net Like 1.4m Follow @CNET

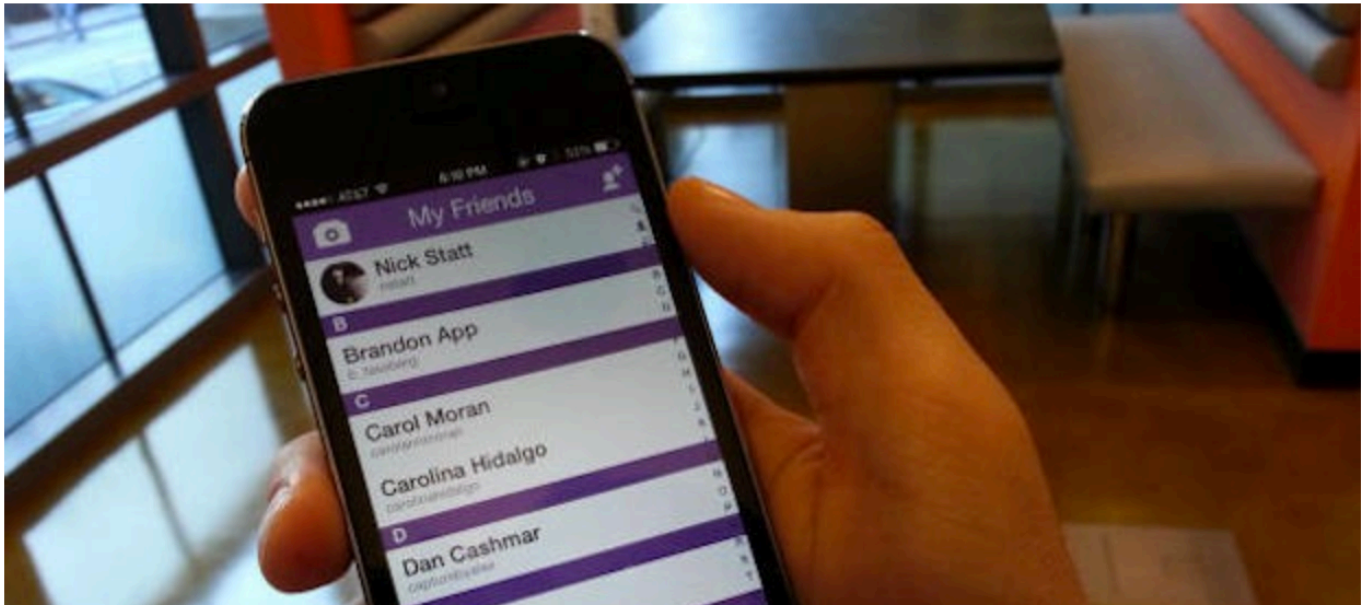
http://news.cnet.com/8301-1009_3-57617034-83/yikes-targets-data-breach-now-could-affect-110m-people/

Researchers publish Snapchat code allowing phone number matching after exploit disclosures ignored

Summary: *Snapchat's previously undocumented API and code for two exploits have been published, allowing mass name/phone number matching, and mass creation of bogus accounts.*

By Violet Blue for Zero Day | December 25, 2013 -- 01:13 GMT (17:13 PST)

Follow @violetblue



http://www.zdnet.com/researchers-publish-snapchat-code-allowing-phone-number-matching-after-exploit-disclosures-ignored-7000024629/

Predictably, Snapchat user database maliciously exposed

Summary: *Snapchat is a textbook example of why responsible disclosure is a failure.*

By Violet Blue for Zero Day | January 1, 2014 -- 18:30 GMT (10:30 PST)

Follow @violetblue

On January 1, 2014, an anonymous user announced the release of SnapchatDB and 4.6 million usernames and matched phone numbers in a Hacker News post.

The Snapchat accounts - even those marked 'private' - were exposed in a database hack that Snapchat knew about for four months, ignored, then told press last week was only "theoretical."

According to SnapchatDB, the leak was made possible with a recently patched, but still useful exploit.

Hacking the database wasn't enough to merit a response

One week ago in December, we broke news that Researchers at Gibson Security published Snapchat code allowing phone number matching after exploit disclosures ignored.

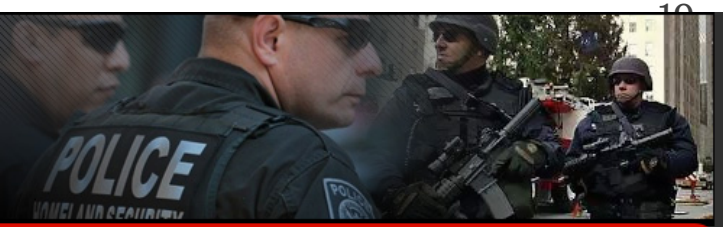
http://www.zdnet.com/predictably-snapchat-user-database-maliciously-exposed-7000024697/

http://malware.dontneedcoffee.com/2013/02/revetoncollectionwinterII.html

NSA INTERNET SURVEILANCE PROGRAM

PRISM

COMPUTER CRIME PROSECUTION SECTION



YOUR COMPUTER HAS BEEN LOCKED!

Your computer has been locked due to suspicion of illegal content downloading and distribution.

The illegal content (414 Mb of photo and video files) was automatically classified as child pornographic materials.

The downloading and ditribution of illigal content, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251 Sexual exploitation of children (Production of child pornography)

18 U.S.C. § 2252 Ceratin activities relating to material involving the sexual explotation of minors (Possession, distribution and receipt of child pornography)

18 U.S.C. § 2252A Ceratin activites relating to material constituing or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 6 month to 10 years and shall be fined up to $250,000.

ALL SUSPICIOUS FILES FROM YOUR COMPUTER WERE TRANSMITTED TO A SPECIAL SERVER AND SHALL BE USED AS EVIDENCES. DON'T TRY TO CORRUPT ANY DATA OR UNBLOCK YOUR COMPUTER IN AN UNAUTHORIZED WAY.

Your case can be classified as occasional/unmotivated, according to 17 (U.S. Code) §512

Thus it may be closed without prosecution.
Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300

green dot MoneyPak

Exchange your cash for a MoneyPak voucher and use your voucher code in the form below:

Code: [ ] SUBMIT

1 2 3 4 5 6 7 8 9 0

Status: Waiting for payment

Permanent lock on 09/28/2013 8:46 p.m. EST

Where can I buy MoneyPak

RITE AID PHARMACY · CVS pharmacy · kmart · 7 ELEVEN · Walgreens · Walmart

Collected technical data

Your IP address: [redacted]
Your host name:
Source or intermediary sites:
Location: [redacted]

Illegal content found:

http://malware.dontneedcoffee.com/2013/08/prism-themed-ransomware.html

Cryptolocker: Menace of 2013

Summary: *The scale of the Cryptolocker threat is disputable. It's the psychology that is truly frightening.*

By Rob O'Neill | December 13, 2013 -- 20:17 GMT (12:17 PST)

Follow @robonz

Security software company Symantec this month named Cryptolocker the "Menace of the Year".

Bitdefender logged over 12,000 victims in a week last month. That's not huge on a global scale but it should be a big enough number to make businesses pay attention.

While relatively few have been affected so far, many of those that have succumbed experienced a world of pain, as the victim stories below will attest.

Backup is the key to recovering from a Cryptolocker lockout.

For anyone who hasn't been paying attention, Cryptolocker is a variant of ransomware that unlike its predecessors does not work by locking a computer. Instead, it encrypts all data and demands a ransom in Bitcoins for the user to regain access.

It is usually distributed as an executable attachment disguised as a Zipped document and presented as an invoice or report or similar via a spam campaign.

All of that would be frightening enough for individual users, but Cryptolocker more than most trojans is a threat to businesses too. that's because it not only attacks data on the PC on which the executable was opened, but also on devices and drives connected to that PC.

http://www.zdnet.com/cryptolocker-menace-of-2013-7000024299/

Så mye koster banktrojanerne

Leif Martin Kirknes
11.04.2013 kl 13:57

Epost

Fem millioner kroner forsvant fra norske bankkonti på grunn av trojanere ifjor, mot 660.000 i 2011.

BEKYMRET: Frank Robert Berg fra Finanstilsynet uroer seg for stadig med avasnerte automatiserte nettbanktrojanere. (Foto: Leif Martin Kirknes)

http://www.idg.no/computerworld/article270128.ece

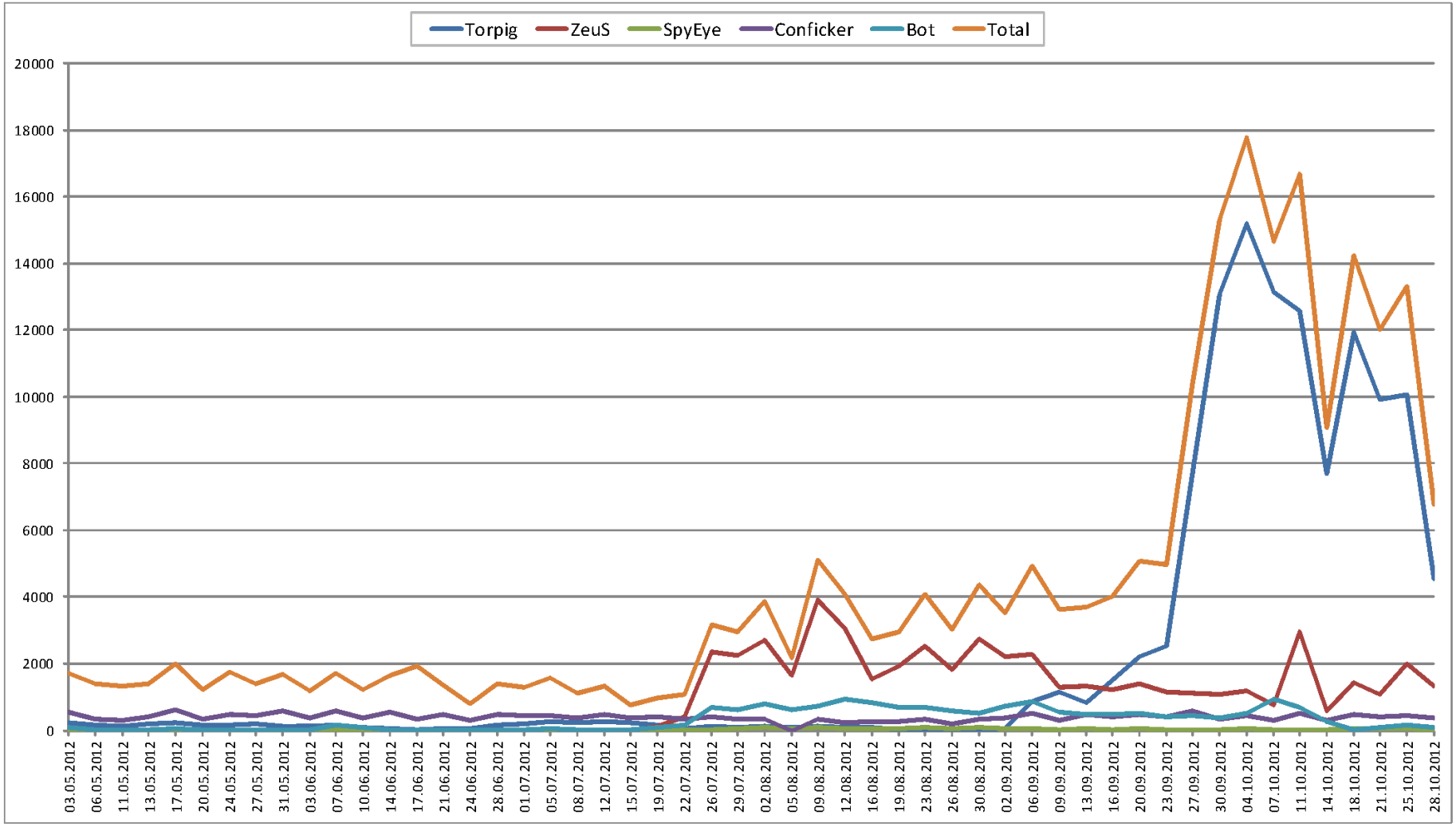
Norske nettsteder sprer skadevare

Leif Martin Kirknes
22.08.2012 kl 07:12

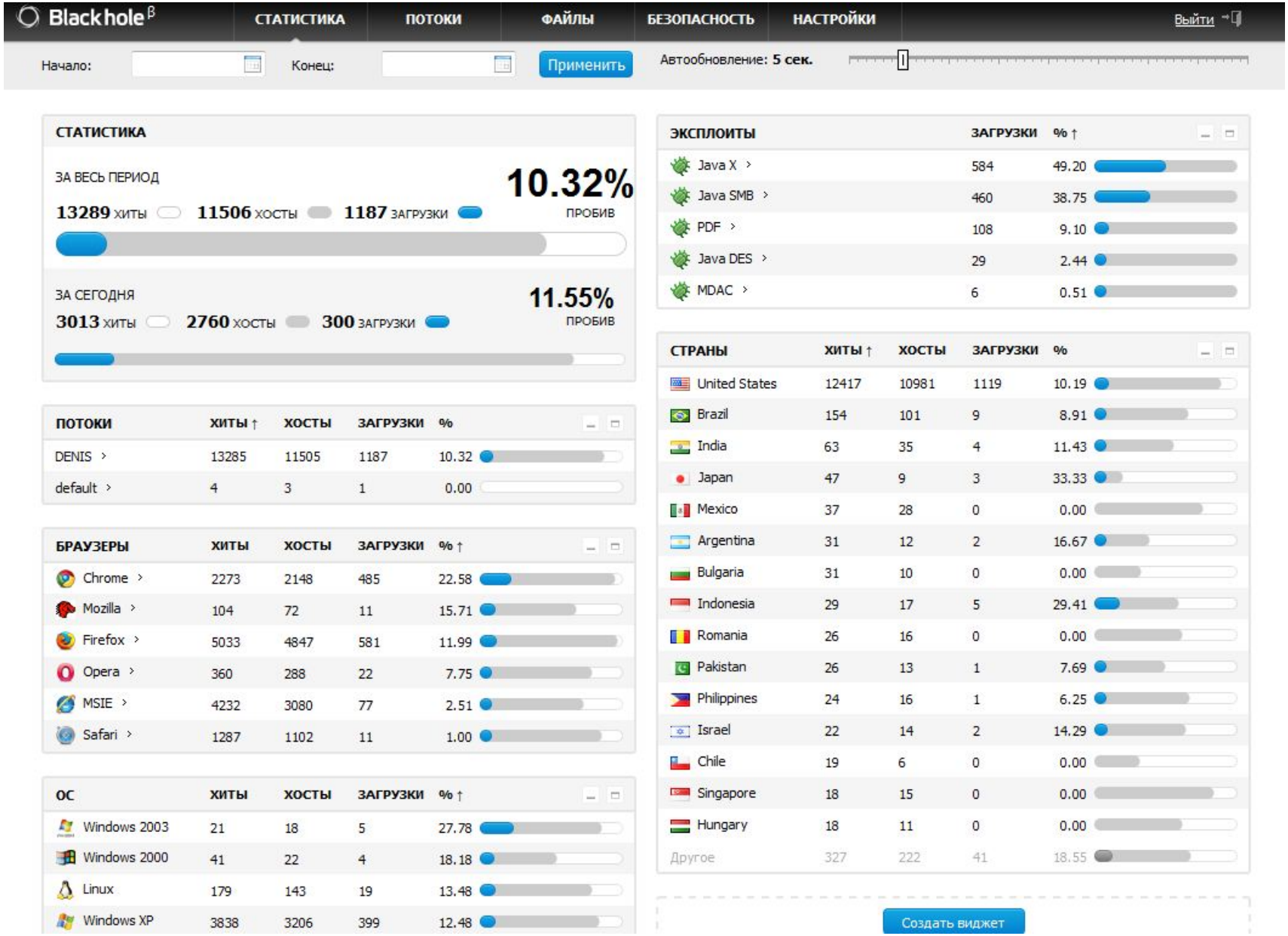
Epost

Stadig flere norske nettsider smitter sine besøkende med ondsinnet programvare. Det melder Norcert.

SMITTEFARE: Marie Moe i Norcert har fått økt tilfang av varsler om infiserte, norske nettsider siste tiden. (Foto: Leif Martin Kirknes)



Statistics from NSM NorCERT on infected clients reported to Norwegian ISPs



http://krebsonsecurity.com/2012/07/new-java-exploit-to-debut-in-blackhole-exploit-kits/

Yahoo malvertising attack linked to larger malware scheme

Cisco found hundreds of related suspicious domains that are probably used to push malware

By **Jeremy Kirk**, IDG News Service | Security

January 09, 2014, 8:48 PM — A deeper look by Cisco Systems into the cyberattack that infected Yahoo users with malware appears to show a link between the attack and a suspicious affiliate traffic-pushing scheme with roots in Ukraine.

Yahoo said on Sunday that European users were served malicious advertisements, or "malvertisements," between Dec. 31 and last Saturday. If clicked, the advertisements directed users to websites that tried to install malicious software.

Cisco discovered that the malicious websites victims landed on are linked to hundreds of others that have been used in ongoing cyberattacks, said Jaeson Schultz, a threat research engineer.

http://www.itworld.com/security/399451/yahoo-malvertising-attack-linked-larger-malware-scheme

INFECTION VECTORS

Java™

OpenX

WordPress

Joomla!™

Ber norske nettbrukere om å skru av Java

Nasjonal sikkerhetsmyndighet (NSM) anbefaler internettbrukere å deaktivere Java i nettleseren etter at det er oppdaget et nytt alvorlig sikkerhetshull.

Fredag 11. januar 2013, kl. 12:38

475

http://www.tv2.no/nyheter/innenriks/ber-norske-nettbrukere-om-aa-skru-av-java-3962939.html

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

China is Behind more than 20 Serious Cyber Attacks against Norway

Norwegian National Security Authority accuses China of computer espionage against Norwegian companies.

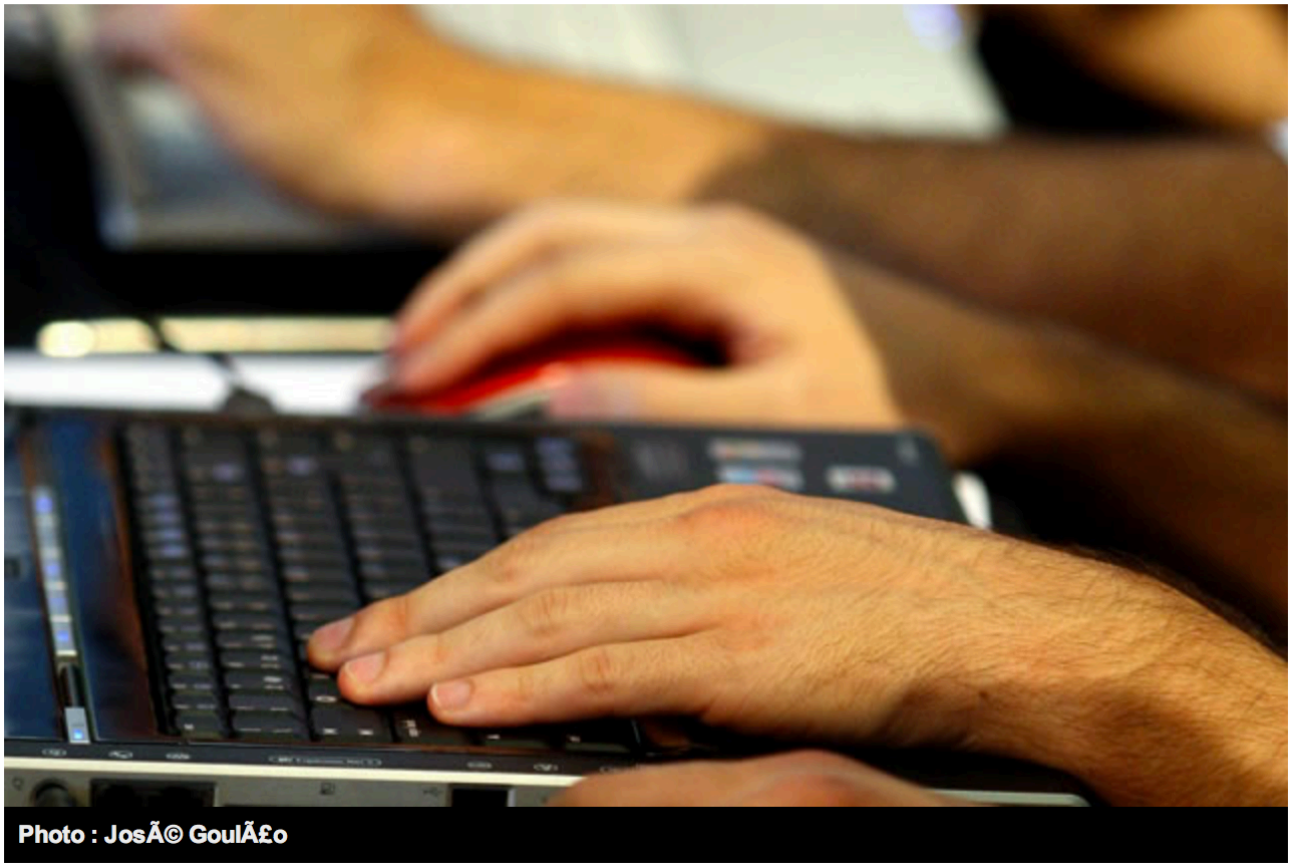
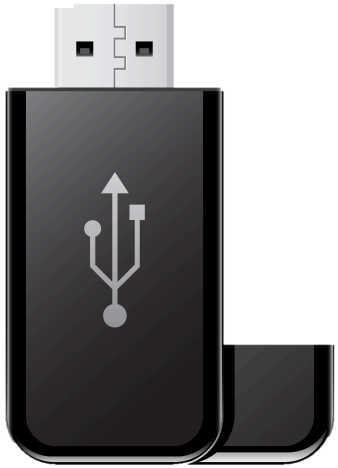


Photo : JosÃ© GoulÃ£o

http://www.tnp.no/norway/politics/3580-china-is-behind-more-than-20-serious-cyber-attacks-against-norway

CROSSING PERIMETERS AND AIR-GAPPED SYSTEMS



Stuxnet's Secret Twin

The real program to sabotage Iran's nuclear facilities was far more sophisticated than anyone realized.

BY RALPH LANGNER | NOVEMBER 21, 2013

http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack

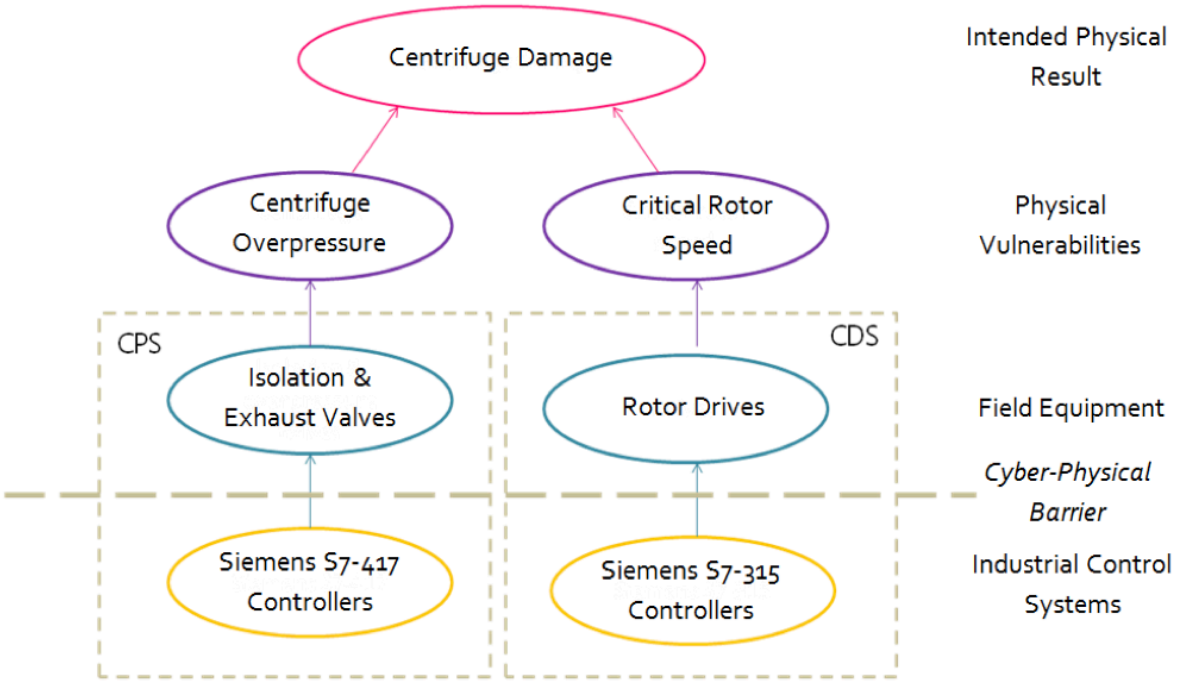
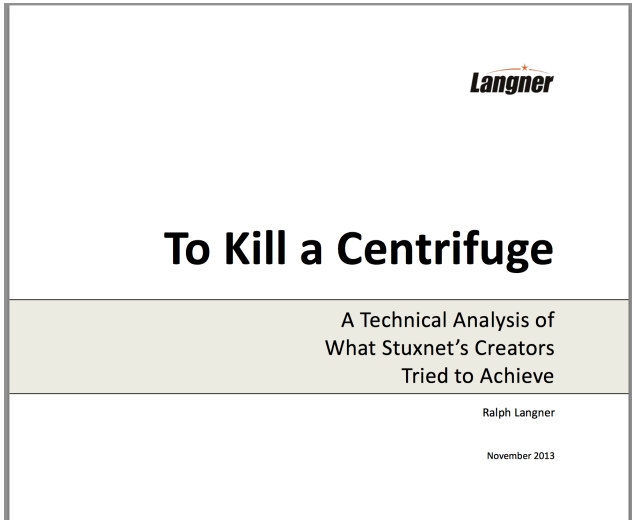


Figure 2: Synopsis of the two different attacks implemented in Stuxnet. Both use a manipulation of industrial control systems to achieve physical damage, exploiting different physical vulnerabilities of the equipment (centrifuge rotors) that basically lead to the same physical result


Langner

To Kill a Centrifuge

A Technical Analysis of
What Stuxnet's Creators
Tried to Achieve

Ralph Langner

November 2013

http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

RAISING AWARENESS John Matherly created the search engine Shodan. He believes he is on the side of good, combating poor security and raising awareness. Video: Øistein Norum Monsen/Dagbladet

Journalists warned system owners and Norwegian NSA of 2500 critical data flaws

How two journalists set out on a mission to test the data security in the whole of Norway.

THERESE DOKSHEIM
tdo@dagbladet.no

http://www.dagbladet.no/2013/12/16/nyheter/nullctrl/shodan/english/english_versions/30861347/

KUNNE IKKE BORTVISE: Rapporten peker på at regjeringens sikkerhetstjeneste ikke hadde myndighet til å bortvise feilparkerte biler. Her går Anders Behring Breivik ut av bombebilen etter å feilparkert den rett utenfor resepsjonen til Høyblokka.

Foto: Overvåkingskamera

DSS får kritikk og skryt i ny 22. juli-evaluering

Departementenes servicesenter (DSS) får i en evalueringsrapport fra PricewaterhouseCoopers (PwC) både ros og ris for sin rolle under håndteringen av terroraksjonen i regjeringskvartalet 22. juli 2011.

http://www.nrk.no/norge/dss-far-kritikk-etter-22.-juli-1.11369000

For 13 of the 15 ministries that are in [regjeringskvartalet], both the main system and back-up were located in the same neighborhood. An even more powerful explosion could effectively have eliminated the newer part of the memory of these ministries.

Excerpt from editorial in Moss Avis 27.10.2011

Already in 2004 the Police Directorate recommended that the street through the government quarter should be closed to traffic to improve security, but it took seven years to get through the bureaucracy.

NRK nyheter. 22.08.2011 http://www.nrk.no/nyheter/norge/1.7760037

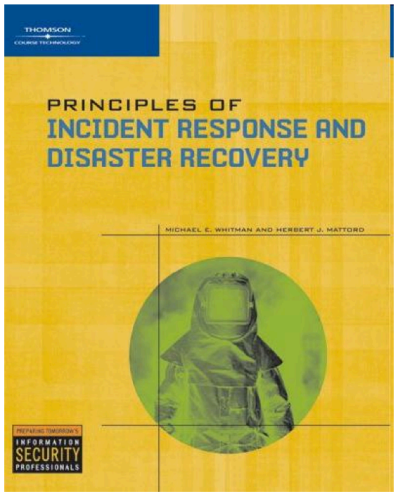
ABOUT THIS COURSE

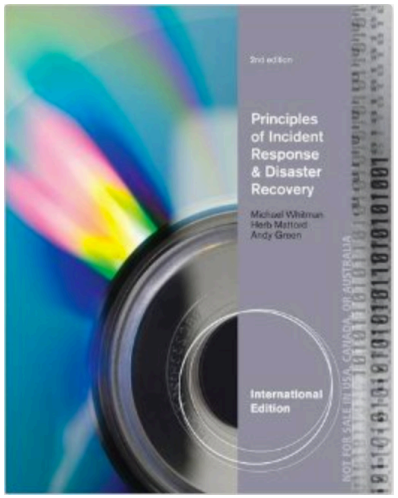
- This course is about preparing for these kinds of incidents and emergencies

- What do you think it requires to be prepared?

LITERATURE

- Michael Whitman and Herbert Mattord: Principles of Incident Response and Disaster Recovery. Thomson, 2007.
- A second edition of the book is also available, I have not yet checked if there are major differences.
- Other literature will be made available for download via the Fronter room.
- *Those of you who have not yet registered for the course, please do so as you will need access to the Fronter room.*





PROJECT WORK

- Group project for IMT3521 (Bachelor)
  - The assignment is to write a contingency plan
  - Group of 2-3 students
- Individual project for IMT4841 (Master)
  - Choose your own topic from the course required reading list
  - Write an in-depth paper on that topic
- For more details read the project guide that will be made available on Fronter

PROJECT APPROVAL AND HAND INNS

- Before you can start with your project topic you have to obtain approval from the instructor
- You should write a half to one page **formal project proposal** and hand it in to me as soon as possible
  - The project proposal will be evaluated and you will get feedback on whether it is approved or declined
- The final project deadline is the **9th of May**
  - You MUST hand in a COMPLETE draft before the **4th of April**

SELF AND PEER EVALUATION

- You have to write an evaluation of your own report
  - The evaluation criteria will be published later
- Your self-evaluation **will count** towards your grade!
- You will also be asked to evaluate the draft of another group/ person using the same criteria
  - This will **not** count towards your grade

IMPORTANT DATES

- Project start:

  As soon as possible!

- COMPLETE DRAFT due: 4th of April
- Project FINAL REPORT due: 9th of May
- Written exam: 28th of May