

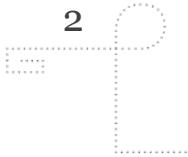


GJØVIK UNIVERSITY COLLEGE

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



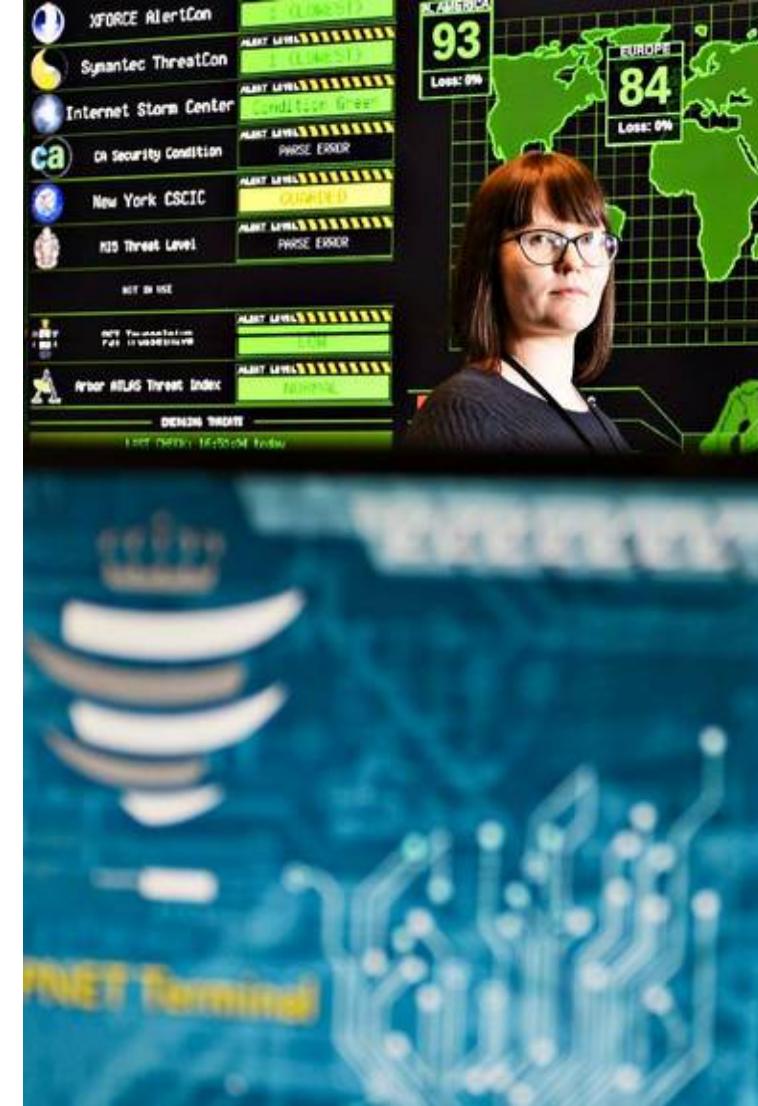


FOTO: ROBERT MCPHERSON, Aftenposten

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

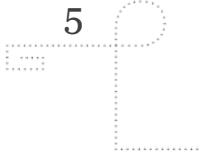




THREATS TO INFORMATION SECURITY

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Technological obsolescence	Antiquated or outdated technologies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...



GJØVIK UNIVERSITY COLLEGE



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](#)

f 1737

1846

```
1. . /$$           /$$           /$$$$$$$  
2. . | $$           | $$           /$$__  $$  
3. . | $$           /$$| $$ /$$$$$$$$$| $$ \_/_ /$$$$$$| /$$$$$$$  
4. . | $$           | $$| $$| $$| ____ /$$/| $$$$/| /$$__  $$| /$$____/  
5. . | $$           | $$| $$| $$| $$ /$$$$/ \_ $$| $$$| $$$| $$$| /$$  
6. . | $$           | $$| $$| $$| $$ /$$/_/ /$$ \ $$| $$| $$| /$$| /$$  
7. . | $$$$$$$$| $$$$/| $$ /$$$$$$$| $$$$/| $$$| $$$| $$$|. $  
8. . | _____/ \____/ | _/| _____/ \____/ | \____/ \____/ \____/  
9.          //Laughing at your security since 2011!  
10.  
11. .-- .-""-.  
12. . ) ( ()  
13. . ( ) ( (   
14. . / ( )  
15. . ( _ _ )          @_, -.-_  
16. . ( _ )_          | _.-._/  
17. . ( )          | lulz..\  
18. . ( __ )          | __--_/  
19. . | ' ' ``\          |  
20. . | [Lulz] \          | /b/  
21. . | \ ,,,---==?A` \ | ,==y'  
22. . _ ,,,---=="\ | [M] \ | ;|\ \ |>  
23. . _ _ \ _ , | H,,---=""bno,  
24. . o 0 ( _ ) ( _ ) \ /          _ AWAW/  
25. . /          _(+)_ dMM/  
26. . \@_ ,,,---=" \ | \ | // MW/  
27. . ---''''          === d/  
28. .          // SET SAIL FOR FAIL!  
29. .          ,  
30. . \ \ \ \ \ , /~~~~~
```

OPERATION: QUISLING

The Norwegian government have chosen to start Data Retention Directive. This meaning they'll keep a track of ALL internet traffic in ALL of Norway, and archive it for up to 6 months.

If this gets through, then other countries will surely follow.



HOW CAN I HELP?

Go to <http://sourceforge.net/projects/loic/> and download the Low Orbit Ion Cannon. Set your URL to number 1 first, then if it goes down, go to number 2. Set method to TCP and threads to 100

Keep firing that fucking cannon

1. www.arbeiderpartiet.no
2. www.hoyre.no

Congratulations,
you are now a part of the army.

SECURITY

Norwegian teens arrested over SOCA DDoS attack

Also accused of pwning online newspaper, financial services group

By John Leyden, 10th May 2012



2,269 followers



12

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.

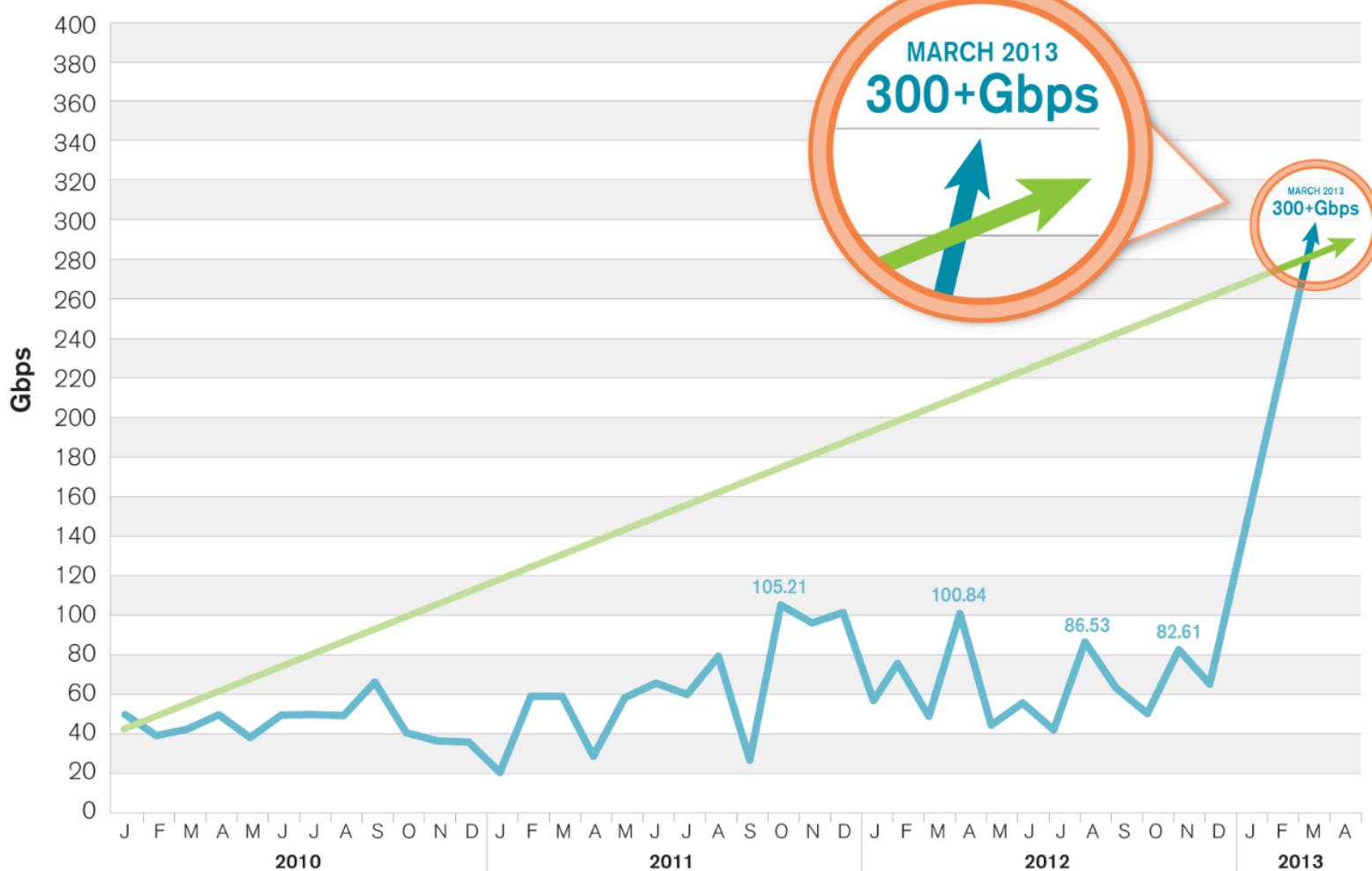
RELATED STORIES

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.

Peak DDoS Attack Size (January 2010-Present)



Source: Arbor Networks, Inc.

ARBOR[®]
NETWORKS

[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.

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

Microsoft Official Blog and Twitter account hacked by Syrian Electronic Army

by Wang Wei on Saturday, January 11, 2014



Sign in

The Official Microsoft Blog

News & Perspectives

TechNet Blogs » The Official Microsoft Blog

[Excerpt View](#) [Full Post View](#)

12Syrian Electronic Army Was Here

a few seconds ago

Syrian Electronic Army Was Here

11Syrian Electronic Army Was Here

a few seconds ago

Syrian Electronic Army Was Here

10Syrian Electronic Army Was Here

a few seconds ago

Syrian Electronic Army Was Here

9Syrian Electronic Army Was Here

a few seconds ago

Syrian Electronic Army Was Here

Search Blogs

Search TechNet with Bing



Search this blog Search all blogs

Microsoft Resources

[Microsoft News Center](#)

[@MSFTNews](#)

Options

About

Email Blog Author

RSS for posts

Atom

Subscribe w/ Email Address

Tags

[Apps](#) [Bing](#) [citizenship](#) [Cloud](#)



Microsoft News @MSFTnews



Follow

Don't use Microsoft emails(hotmail,outlook), They are monitoring your accounts and selling the data to the governments. #SEA
@Official_SEA16

Reply

Retweet

Favorite

More

145

RETWEETS

30

FAVORITES



12:33 AM - 12 Jan 14



Xbox Support (1-5) 
@XboxSupport

Guinness World Record Holder: Most Responsive Brand on Twitter!
Hours: Mon-Fri 6am-12am PT & Sat-Sun 9am-6pm
Redmond, WA · support.xbox.com

1,514,238 TWEETS	205,307 FOLLOWING	356,840 FOLLOWERS
---------------------	----------------------	----------------------

 Followed by Microsoft Support.

Tweets All / No replies

 **Xbox Support (1-5)** @XboxSupport 2m
Syrian Electronic Army Was Here via @Official_SEA16 #SEA
[Expand](#) [Reply](#) [Retweet](#) [Favorite](#) [More](#)

 **Xbox Support (1-5)** @XboxSupport 3m
Syrian Electronic Army was here via @Official_SEA 16 #SEA
[Expand](#) [Reply](#) [Retweet](#) [Favorite](#) [More](#)

 **Xbox Support (1-5)** @XboxSupport 7m
SEA xbx.lv/1dEJ5Xw

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



8+1



190



More +

Comments

112



(Credit: Target)

Target's data breach is much broader than once believed.

The nationwide retailer on Friday announced



1.4m



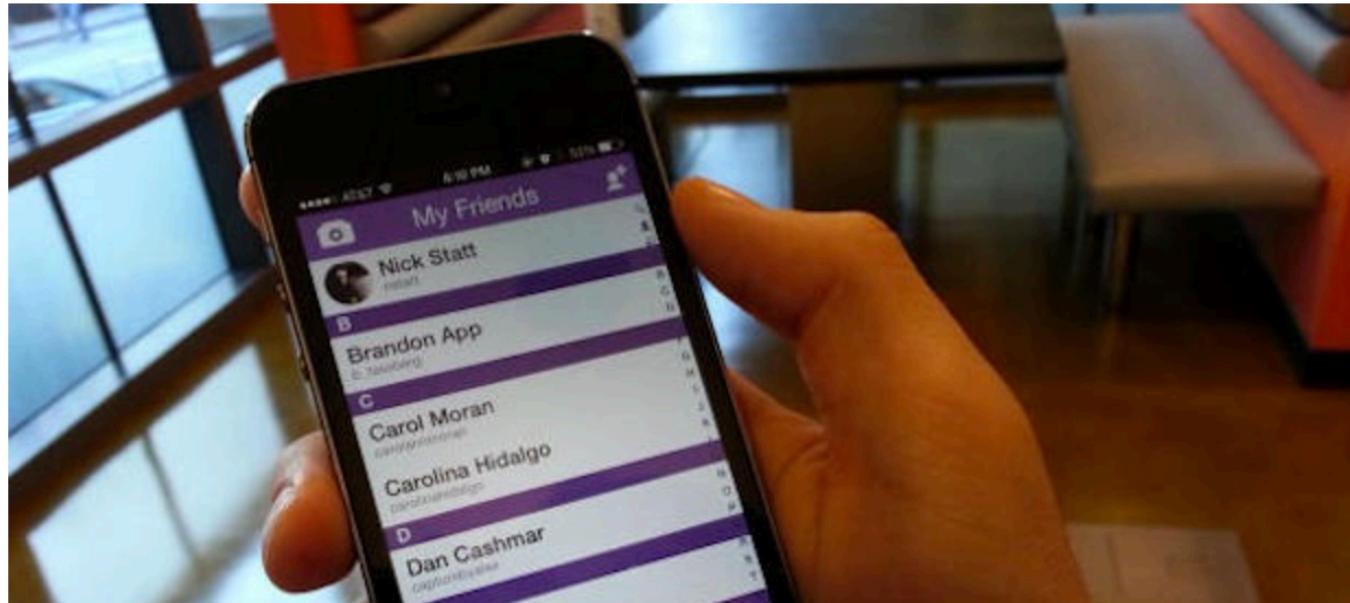
Researchers publish Snapchat code allowing phone number matching after exploit disclosures ignored

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](#)



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](#).

The screenshot shows a landing page for "SnapchatDB". At the top, it says "Bringing 4.6 million users' information to your fingertips". Below that is a large button labeled "Download the database" with two options: "As SQL dump" and "As CSV file". To the right of the download button, there's a section titled "What am I downloading?". It explains that the data includes 4.6 million users' phone number information along with their usernames. It also mentions that people tend to use the same username around the web so you can use this information to find phone number information associated with Facebook and Twitter accounts, or simply to figure out the phone numbers of people you wish to get in touch with. At the bottom, there are links to "See a detailed view of the available area codes" and "See a sample of the available data".

POLITIET
INSTITUTT FOR CYBERCRIME

Deres IP-adresse: [REDACTED]
Deres Internettleverandør: [REDACTED]
Oppholdssed: Norway, [REDACTED]

DATAMASKINEN DIN ER LÅST

Datamaskinen din er midlertidig låst på grunn av uautorisert datavirksomhet.

Det er mulige brudd du har begått:

Art 174. Opphavsrettsbrudd
Straffes med fengsel fra 2 til 5 år eller bot som beløper seg fra 100 000 opp til 120 000 NOK. (Bruk eller distribusjon av verk beskyttet med opphavsrett)

Art 183. Pornografi
Straffes med fengsel fra 2 til 3 år eller bot som beløper seg fra 100 000 opp til 120 000 NOK. (Bruk eller distribusjon av pornografiske filer)

Art 184. Pornografisk produksjon hvor barn deltar (barna under 18 år)
Straffes med fengsel fra 10 til 15 år eller bot som beløper seg fra 125 000 opp til 320 000 NOK. (Bruk eller distribusjon av pornografiske filer)

Art 104. Popularisering av terrorisme
Straffes med fengsel inntil 25 år uten klagerrett eller bot som beløper seg fra 300 000 opp til 420 000 NOK med inndragning av eiendom. (Du har besøkt hjemmesider til terroristiske organisasjoner)

Art 68. Spredning av virus programvare
Straffes med fengsel inntil 2 år eller bot som beløper seg fra 90 000 opp til 165 000 NOK. (Etablering eller spredning av virus programvare som fører til ødeleggelse av datamaskinen)

Art 113. Bruk av ulisensiert programvare
Straffes med fengsel inntil 2 år eller bot som beløper seg fra 85 000 opp til 115 000 NOK. (Bruk av ulisensiert programvare)

Art 99. Svindel med betalingskort, carding
Straffes med fengsel inntil 5 år eller bot som beløper seg fra 185 000 opp til 320 000 NOK med inndragning av eiendom. (Transaksjon med bruk av betalingskort som ikke var innsatt eller bekreftet av kortholderen)

Art 156. Distribusjon av spam-meldinger med pornografisk innhold
Straffes med fengsel inntil 2 år eller bot som beløper seg fra 72 000 opp til 200 000 NOK. (Distribusjon av spam-meldinger med pornografisk innhold via e-post eller sosialt nettverk)

HVIS DU PRØVER Å FJERNE BLOKKERING AV DATAMASKINEN SELV, VIL ALLE DINE DATA VÆRE FORMATERT BORTSETT FRA FILER SOM BEVISER ULOVIGE HANDLINGER.

ALLE ULOVIGE HANDLINGER SOM SKJER PÅ DIN DATAMASKIN INKLUDERT BILDER OG VIDEOER FRA WEB-KAMERA, ER REGISTRERT I POLITIETS DATABASE FOR YTTERLIGERE IDENTIFIKASJON AV DIN IDENTITET. POLITIET HAR REGISTRERT PÅ DIN DATAMASKIN VISNING AV PORNOGRAFISKE FILER HVOR MINDREÅRIGE DELTAR.

Video-opptak: På

Ukash or **paysafecard**

Du kan få Ukash fra hundretusener av globale lokasjoner, online, fra lommebøker, fra kiosker og minibanker.

Bytter kontanter for Ukash kupong og skriv inn kupongkoden i skjemaet nedenfor.

Koden: BEKREFTET

1 2 3 4 5 6 7 8 9 0

Status: Waiting for betaling 47:59:34

Hvor jeg kan kjøpe Ukash kuponger

Det første bruddet kan ikke medføre straffesvar, men kun betaling av en bot med hjemmel i lov om lojalitet til befolkning, vedtatt 29 januar 2013. Ved gjentatte brudd blir straffesvar unngåelig.

ETTER BETALING AV BOTEN BLIR DATAMASKINEN DIN LÅST OPP.

Vennligst vær oppmerksom på at boten må betales kun innen 48 timer. Hvis du ikke gjør dette innen denne fristen, blir det ikke mulig å låse opp datamaskinen din.

I det tilfelle blir det automatisk anlagt en straffesak mot deg.

Med formål å gjøre politiarbeidet mer effektivt og for å forbedre prosess av datakriminelles identifikasjon, ble 29. januar 2013 inngått en internasjonal avtale med selskap som utvikler anti-virus programvare.



NSA INTERNET SURVEILLANCE 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 distribution of illegal 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 Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)

18 U.S.C. § 2252A Certain activities relating to material constituting 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.**

Collected technical data

Your IP address:

Your host name:

Source or intermediary sites:

Location:

Illegal content found:



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) 5512

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**



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

Code:

1 2 3 4 5 6 7 8 9 0 ➔

SUBMIT

Status: Waiting for payment

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



Where can I buy MoneyPak



Walgreens

Walmart

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.

connected to that PC.

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

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)



Norske nettsteder sprer skadevare



Leif Martin Kirknes
22.08.2012 kl 07:12

Epost

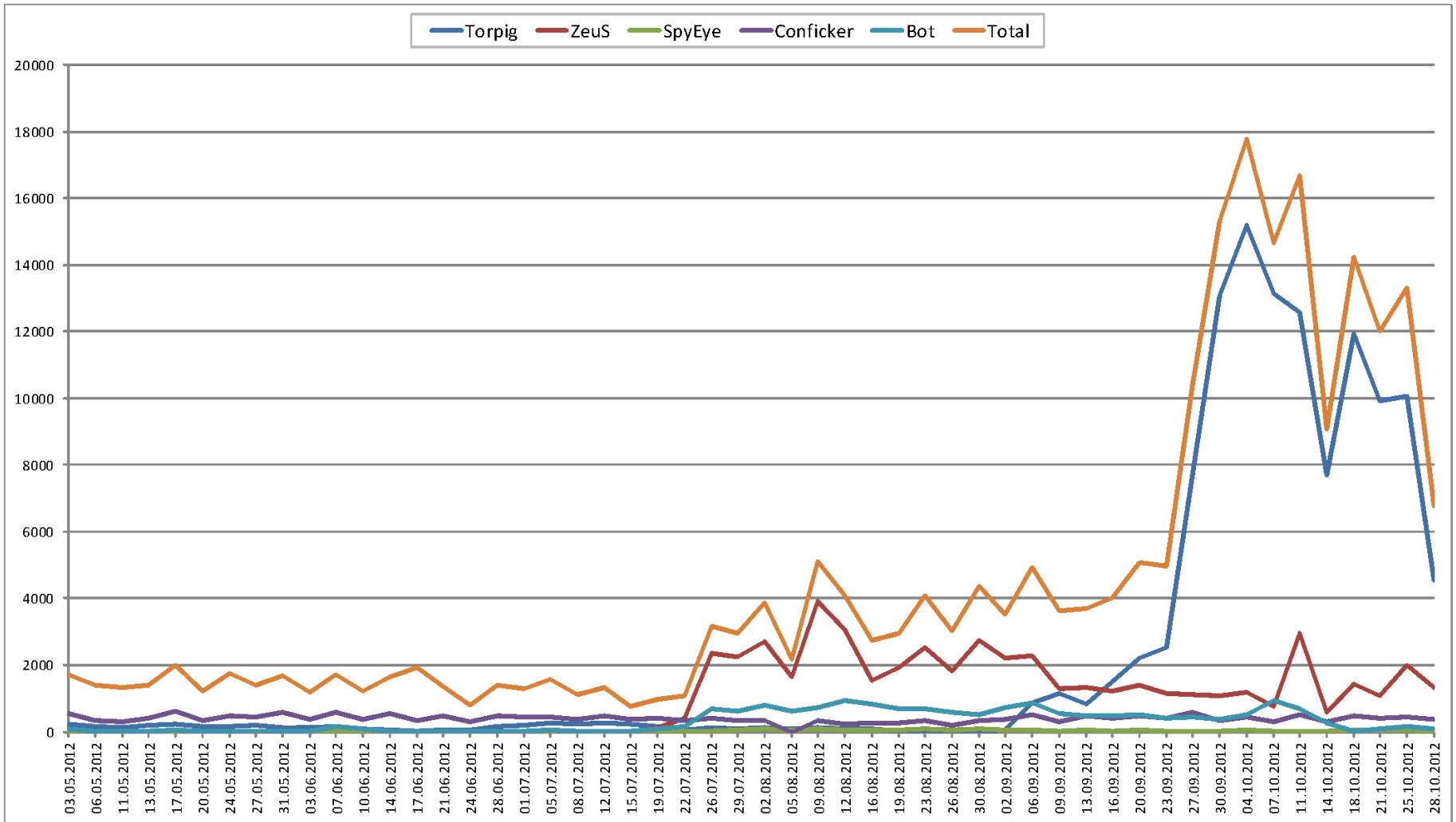


Stadig flere norske nettsider smitter sine besøkende med ondsinnet programvare. Det melder Norcert.



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





Statistics from NSM NorCERT on infected clients reported to Norwegian ISPs

Начало:

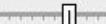


Конец:



Применить

Автообновление: 5 сек.



СТАТИСТИКА

ЗА ВСЮ ПЕРИОД

10.32%

ПРОБИВ

13289 хиты 11506 хосты 1187 ЗАГРУЗКИ

ЗА СЕГОДНЯ

11.55%

ПРОБИВ

3013 хиты 2760 хосты 300 ЗАГРУЗКИ

ПОТОКИ

ХИТЫ ↑

ХОСТЫ

ЗАГРУЗКИ

%

DENIS >

13285

11505

1187

10.32

default >

4

3

1

0.00

БРАУЗЕРЫ

ХИТЫ

ХОСТЫ

ЗАГРУЗКИ

%

Chrome >

2273

2148

485

22.58

Mozilla >

104

72

11

15.71

Firefox >

5033

4847

581

11.99

Opera >

360

288

22

7.75

MSIE >

4232

3080

77

2.51

Safari >

1287

1102

11

1.00

ОС

ХИТЫ

ХОСТЫ

ЗАГРУЗКИ

%

Windows 2003

21

18

5

27.78

Windows 2000

41

22

4

18.18

Linux

179

143

19

13.48

Windows XP

3838

3206

399

12.48

ЭКСПЛОИТЫ

ЗАГРУЗКИ

%

Java X >

584

49.20

Java SMB >

460

38.75

PDF >

108

9.10

Java DES >

29

2.44

MDAC >

6

0.51

СТРАНЫ

ХИТЫ ↑

ХОСТЫ

ЗАГРУЗКИ

%

United States

12417

10.19

Brazil

154

8.91

India

63

11.43

Japan

47

33.33

Mexico

37

0.00

Argentina

31

16.67

Bulgaria

31

0.00

Indonesia

29

29.41

Romania

26

0.00

Pakistan

26

7.69

Philippines

24

6.25

Israel

22

14.29

Chile

19

0.00

Singapore

18

0.00

Hungary

18

0.00

Другое

327

18.55

Создать виджет

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.



INFECTION VECTORS





Ber norske nettbrukere om å skru av Java

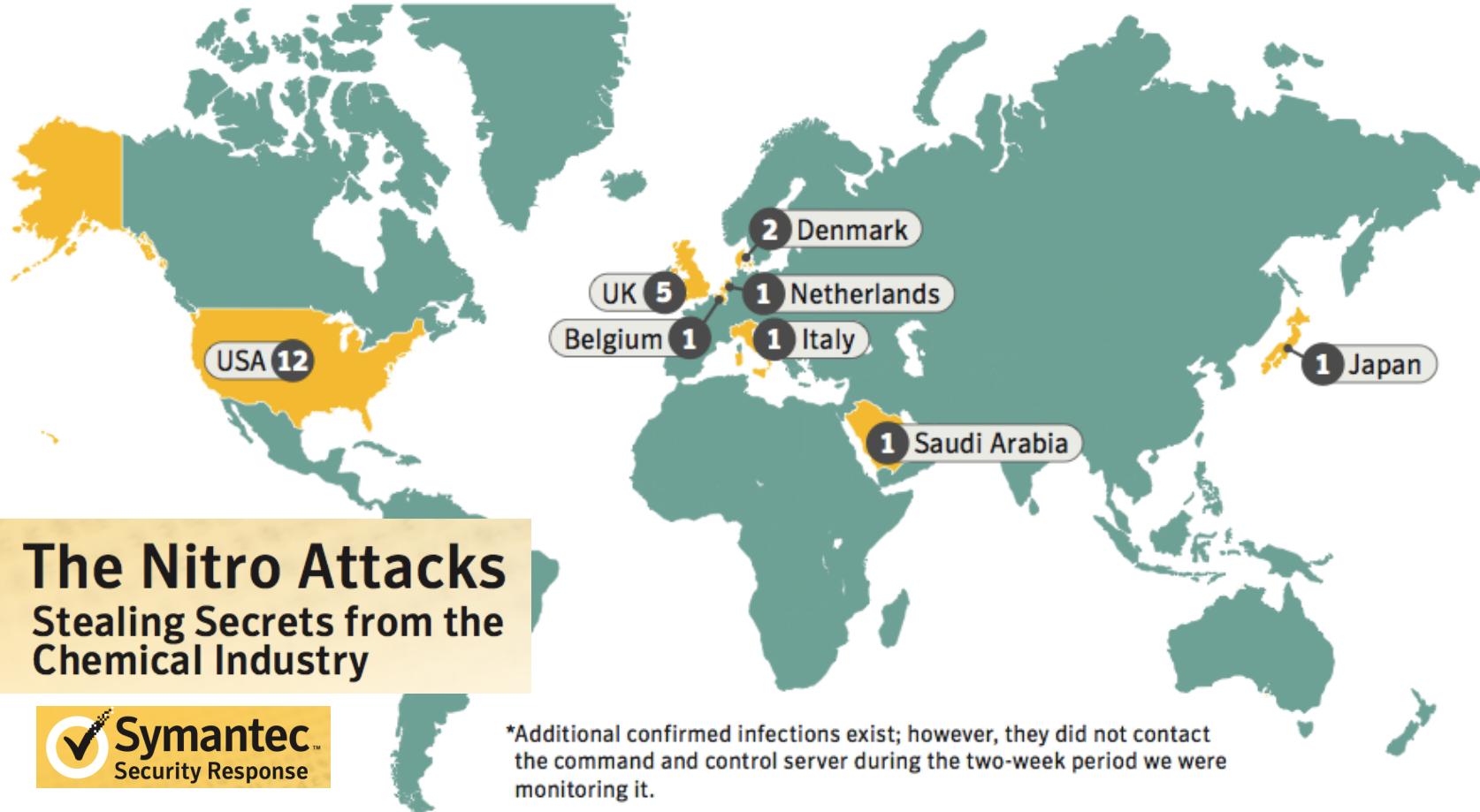
Nasjonal sikkerhetsmyndighet (NSM) anbefaler internettbrukere å deaktivere Java i nettleseren etter at det er oppdaget et nytt alvorlig sikkerhetshull.

Fredag 11. januar 2013, kl. 12:38





Country of origin of targeted organizations*



OBSERVED GLOBAL APT1 ACTIVITY



China is Behind more than 20 Serious Cyber Attacks against Norway

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

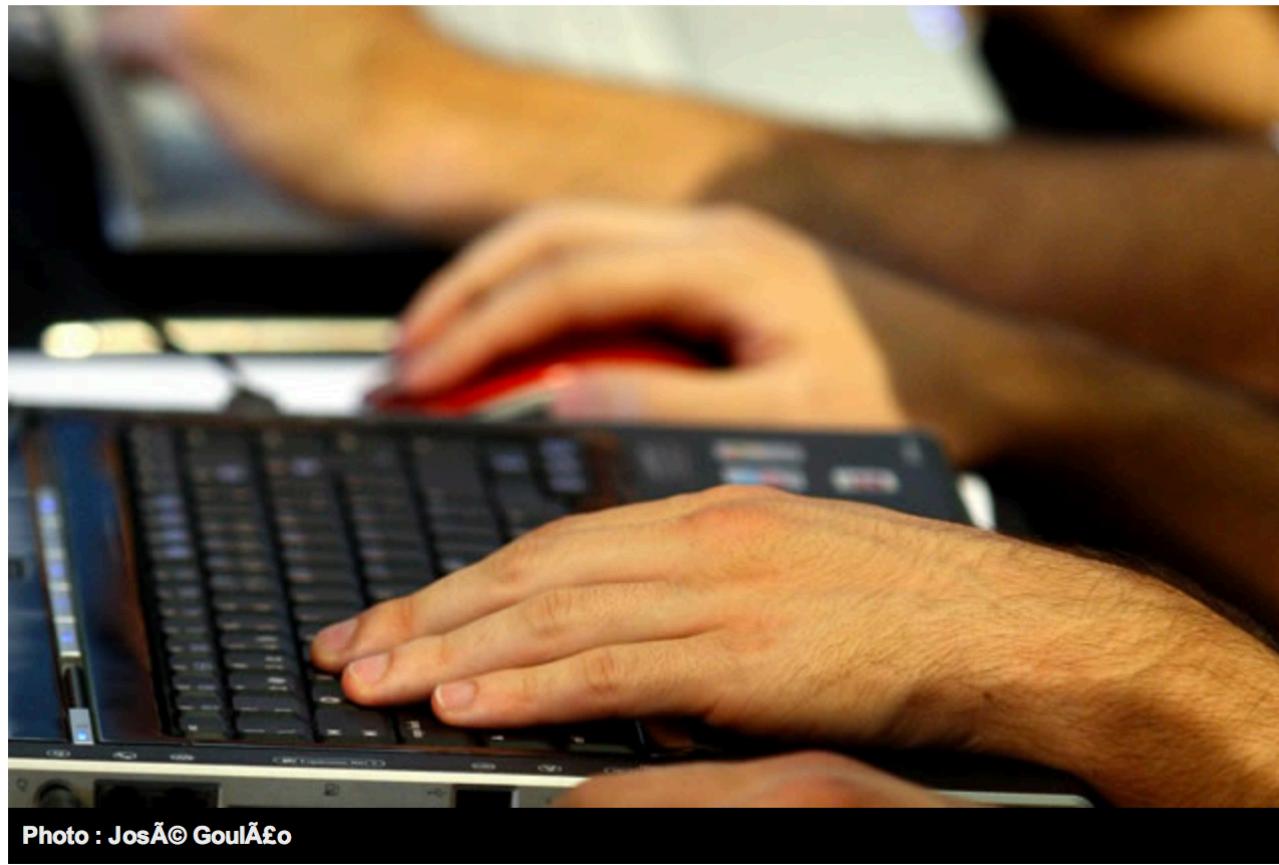
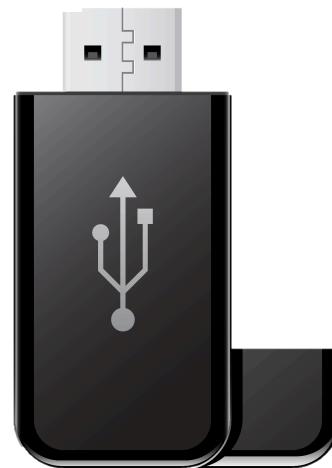


Photo : Jos© Gouli©



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



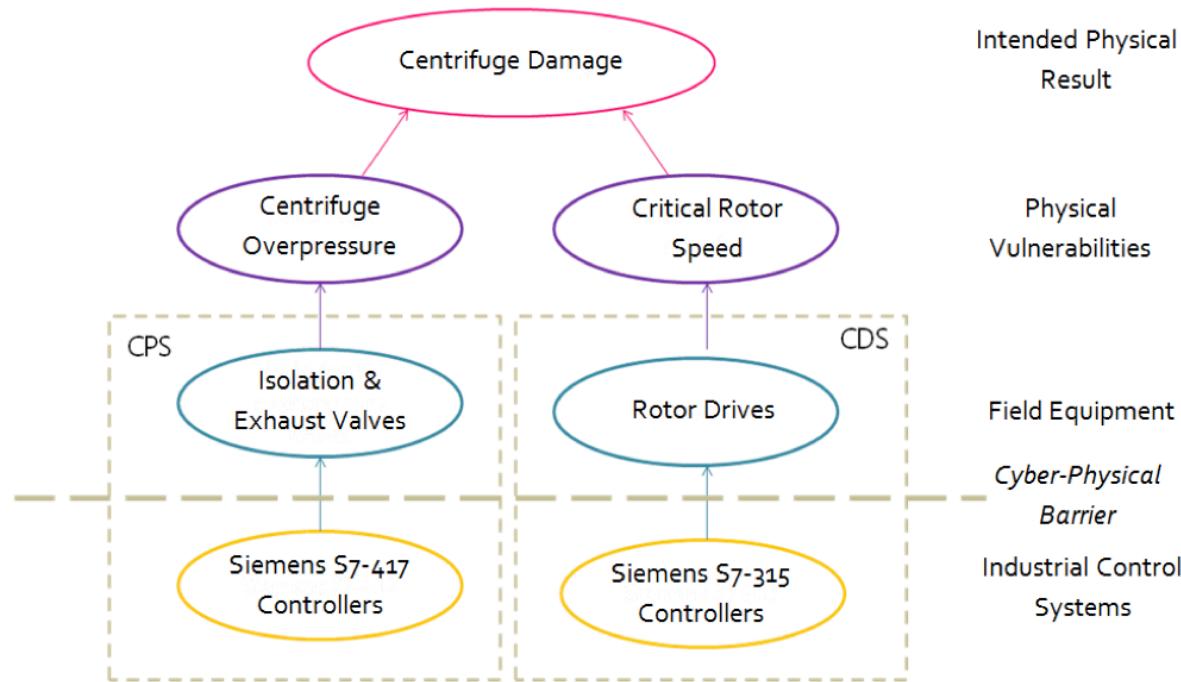


Figure 2: Synopsis of the two different attacks implemented in Stuxnet. Both use a manipulation of industrial control systems to achieve physical damage, exploiting different physical vulnerabilities of the equipment (centrifuge rotors) that basically lead to the same physical result

To Kill a Centrifuge

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

Ralph Langner

November 2013



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.



THERÈSE DOKSHEIM
tdo@dagbladet.no



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.



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

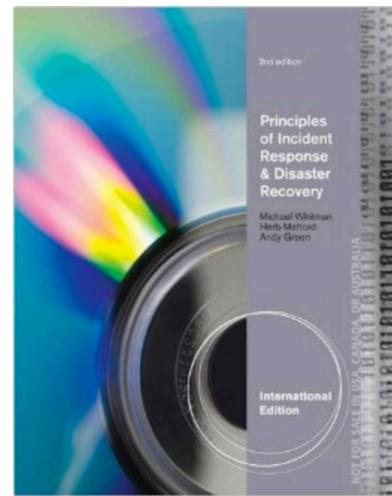
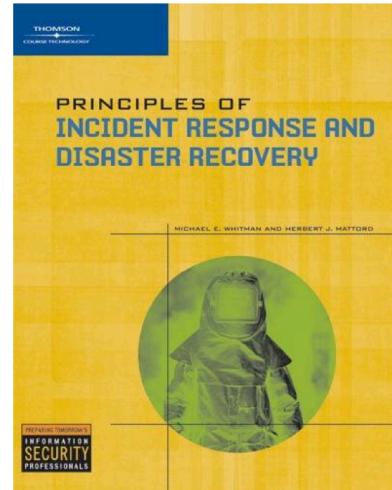
- This course is about preparing for these kinds of incidents and emergencies
- What do you think it requires to be prepared?





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.*

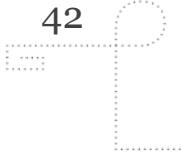




PROJECT WORK

- 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

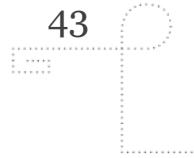




PROJECT APPROVAL AND HAND INNS

- 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**

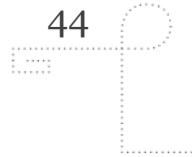




SELF AND PEER EVALUATION

- 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

