Breakfast Seminars in Information Security

# Digital warfare or organized crime

PRO.M.IS
security built in

**(Professional Master in Information Security)**

Dr. Anders Carlsson, (anders.carlsson@bth.se)

# Anders Carlsson

25y Royal Swedish Navy
ÖrlKn (Lt Cmd)
Submarines
< 20year in BTH teacher & researcher
Phd in Cyber Security from
National University of Radio Electronics
Kharkiv Ukraine
last years [www.engensec.eu](http://www.engensec.eu) to develop a

Msc in Cyber Security

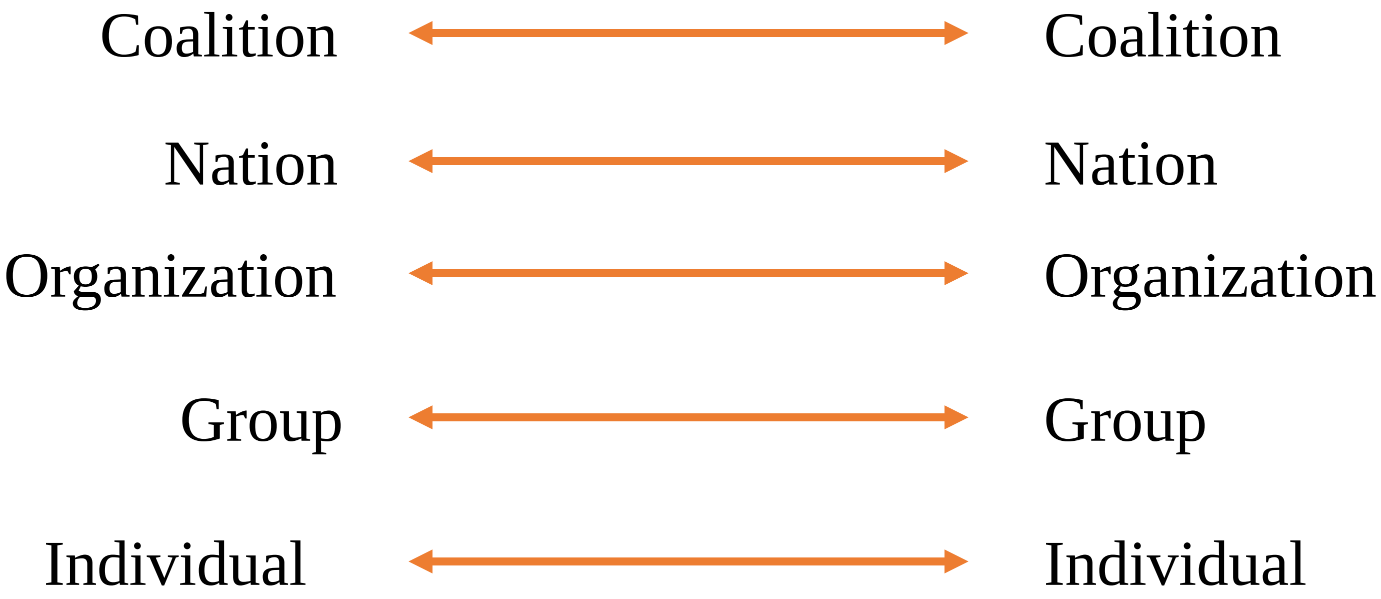
EU + Ukraine + Russia

# agenda

- The last year’s changed threat against the countries, companies and organizations.

- PROMIS general information
- Courses
- How to apply

# Actors then threat opponent……



Coalition ↔ Coalition

Nation ↔ Nation

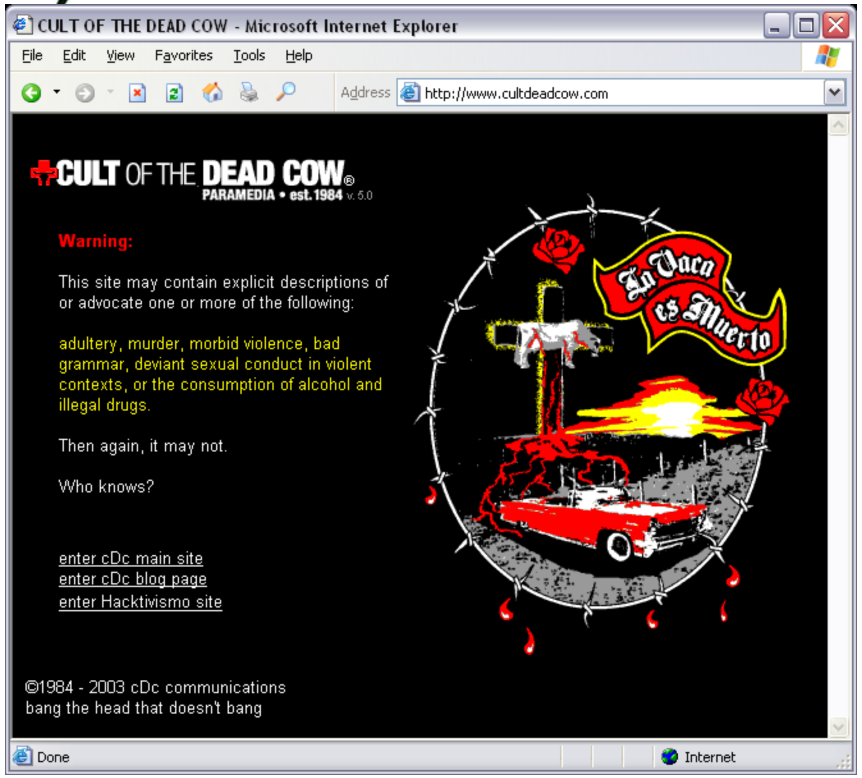
Organization ↔ Organization

Group ↔ Group

Individual ↔ Individual

# From Hacktivism →
organized crime that make BIG money
→using **Hybrid War to overtake a** country

I managed to take over Georgia 2008, Crimea 2014 and manipulate US-election 2016, nobody stop me



CULT OF THE DEAD COW - Microsoft Internet Explorer

Address http://www.cultdeadcow.com

CULT OF THE DEAD COW®
PARAMEDIA • est. 1984 v. 5.0

Warning:

This site may contain explicit descriptions of or advocate one or more of the following:

adultery, murder, morbid violence, bad grammar, deviant sexual conduct in violent contexts, or the consumption of alcohol and illegal drugs.

Then again, it may not.

Who knows?

enter cDc main site
enter cDc blog page
enter Hacktivismo site

©1984 - 2003 cDc communications
bang the head that doesn't bang

La Vaca es Muerto
Done
Internet

LIKE THE WATERGATE BREAK-IN...
ONLY THIS TIME IT'S BY A RUSSIAN PRESIDENT.
HACKING INTO DNC CAMPAIGN FILES
ENTER
PUTIN
I'M 4 TRUMP
©DAVEGRANLUND.COM
POLITICALCARTOONS.COM

# Threat Report, Survey, from

- CrowdStrike
- ESET
- KasperskyLab
- EMISOFT

shows a **dramatically increase in ransomware** attack against:

- companies
- municipal
- governments and
- agencies
- healthcare providers

**A town in Florida has paid $500,000 (£394,000) to hackers after a ransomware attack**

Lake City voted to pay hackers in $??? In Bitcoin
after two weeks downed computer

Coastal suburb Riviera Beach **recently paid hackers $600,000** following a similar incident that locked municipal staff out of important files.

**The cyber-attack that sent an Alaskan community back in time**

# US-Security reports shows that during  2019

966 government agencies, educational establishments and healthcare providers at a potential cost in excess of $7.5 billion.

113 state and municipal governments and agencies.
764 healthcare providers.
89 universities, colleges

**A town in Florida has paid $500,000 (£394,000) to hackers after a ransomware attack**

Lake City voted to pay hackers in $??? In Bitcoin
after two weeks downed computer

Coastal suburb Riviera Beach **recently paid hackers $600,000** following a similar incident that locked municipal staff out of important files.

**The cyber-attack that sent an Alaskan community back in time**

# Change Cold war BI company

# “Dark Basin”

- A hack-for-hire group targeted thousands of people and hundreds of organizations across six continents for several years, according to a report by Citizen Lab.
   dubbed “Dark Basin”, with high confidence to an Indian company called BellTroX InfoTech Services.

**SaaS**

***Spy-as-a-service***

**CaaS**

***Cybercrime-as-a-service***

**FaaS**

***Fraud-as-a-service***

000

*the greedy got greedier*

**BGH**

***big-game-hunting***

**RaaS**

***ransomware-as-a-service***

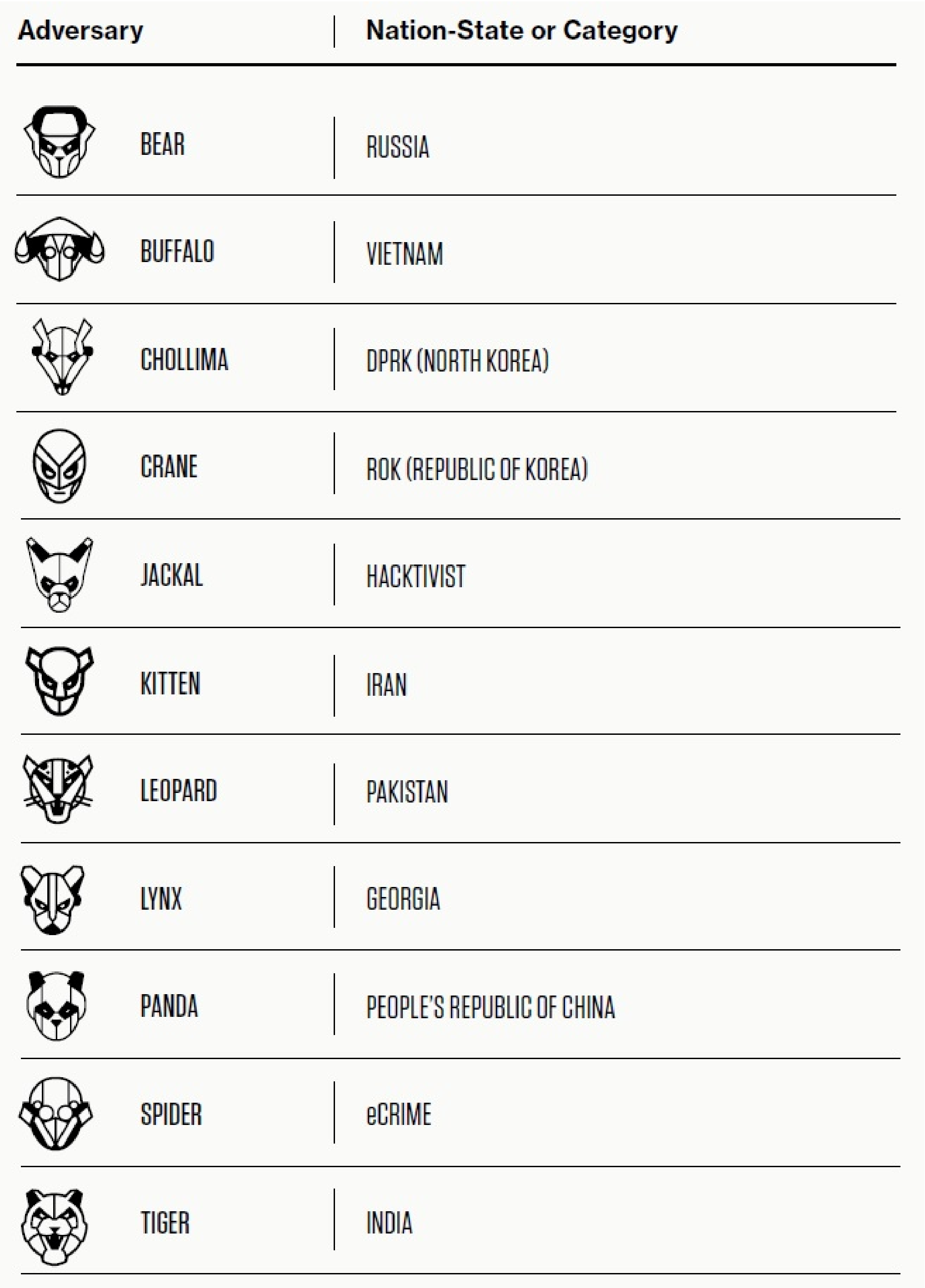
**MaaS**

***Malware-as-a-service***

***To Pay or not to Pay***

# Who is behind these attacks

https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1864660085



| Adversary | Nation-State or Category |
|---|---|
| BEAR | RUSSIA |
| BUFFALO | VIETNAM |
| CHOLLIMA | DPRK (NORTH KOREA) |
| CRANE | ROK (REPUBLIC OF KOREA) |
| JACKAL | HACKTIVIST |
| KITTEN | IRAN |
| LEOPARD | PAKISTAN |
| LYNX | GEORGIA |
| PANDA | PEOPLE'S REPUBLIC OF CHINA |
| SPIDER | eCRIME |
| TIGER | INDIA |

# CryptoLocker 2013 – 2014
# ~0.5 Milj payed 400$ ( 2 btc -> 0.3 btc)
# PostNord attack

- From a simple to a  very anvanced ransomware within 4-5 month

5 treads ,

- phone-home,
- inhibit AV software,
- creating a bitcoin wallet
- Encryption of files
- examine the network and infect other computers

estimated 50-90 developer in staff

# PLA Unit 61398

a.k.a. APT 1, Comment Crew, Comment Panda, GIF89a, and Byzantine Candor

**P**eople's **L**iberation Army: **A**dvanced **P**ersistent **T**hreat unit that has been alleged to be a source of Chinese computer hacking attacks in Pudong, Shanghai.

- From left, Chinese military officers
  Gu Chunhui,
  Huang Zhenyu,
  Sun Kailiang,
  Wang Dong, and
  Wen Xinyu

- have been indicted on cyber espionage charges
  source FBI: https://www.fbi.gov/news/stories/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s

# GRU - Unit 29155

After speaking critically about what he saw as corruption within the Russian government, he fled retribution to the UK, where he remained a vocal critic of the Russian state. Six years after fleeing, he was poisoned by two Russians in a suspected assassination.

- Poisoning of Alexander Litvinenko 2006. with polonium-210

Poisoning of Sergei and Yulia Skripal was also a target of Unit 29155

# Unit 29155,Unit 26165, Unit 74455, Iron Viking a Top-Secret Russian Intelligence Unit´s

- has the task to

  *Destabilize Europe* using:

  The Hybrid Warfare

The combined use of

PSYOPS, propaganda and cyberwarfare

in Geopolitical and Military operations

are hallmarks of Russian “hybrid warfare.”

WAIT, I'M HAVING A LITTLE TROUBLE BREATHING.
MOTHER RUSSIA
CRIMEA
WAIT TILL YOU TRY SPEAKING.-

2014

Russian GRU's Main Center for Special Technologies (GTsST), also known as

# Military -Unit 74455 -Unit 29155 -Unit 26165

*other name used by them self – Battalion Iron Viking*

- a.k.a Sandworm, Fancy Bear, APT28, Pawn Storm, Sofacy Group (by Kaspersky), Sednit, Tsar Team (by FireEye) and STRONTIUM (by Microsoft)) is a Russian cyber espionage group.

Sandworm / Fancy Bear is thought to be responsible for cyber attacks on: the German parliament, the French television station TV5Monde, the White House, NATO, the Democratic National Committee, the Organization for Security and Co-operation in Europe, the campaign of French presidential candidate Emmanuel Macron.

The group promotes the political interests of the Russian government,
Among other things, it uses zero-day exploits, spear phishing and malware to compromise targets.

TOOLS: BadRabbit, BlackEnergy, GCat, GreyEnergy, Industroyer, KillDisk, NotPetya, PSCrypt, TeleBot, TeleDoor, xData

# *PsyOps and Ifrastructure attacks by SANDWORM*

- BlackEnergy discovered 2007 and used  2008 during Russia's intervention in Georgia attack infrastructure.

  BlackEnergy 2 was discovered in year 2010. The code was rewritten, which made the program more sophisticated.  From 2013 supports 64-bit systems.

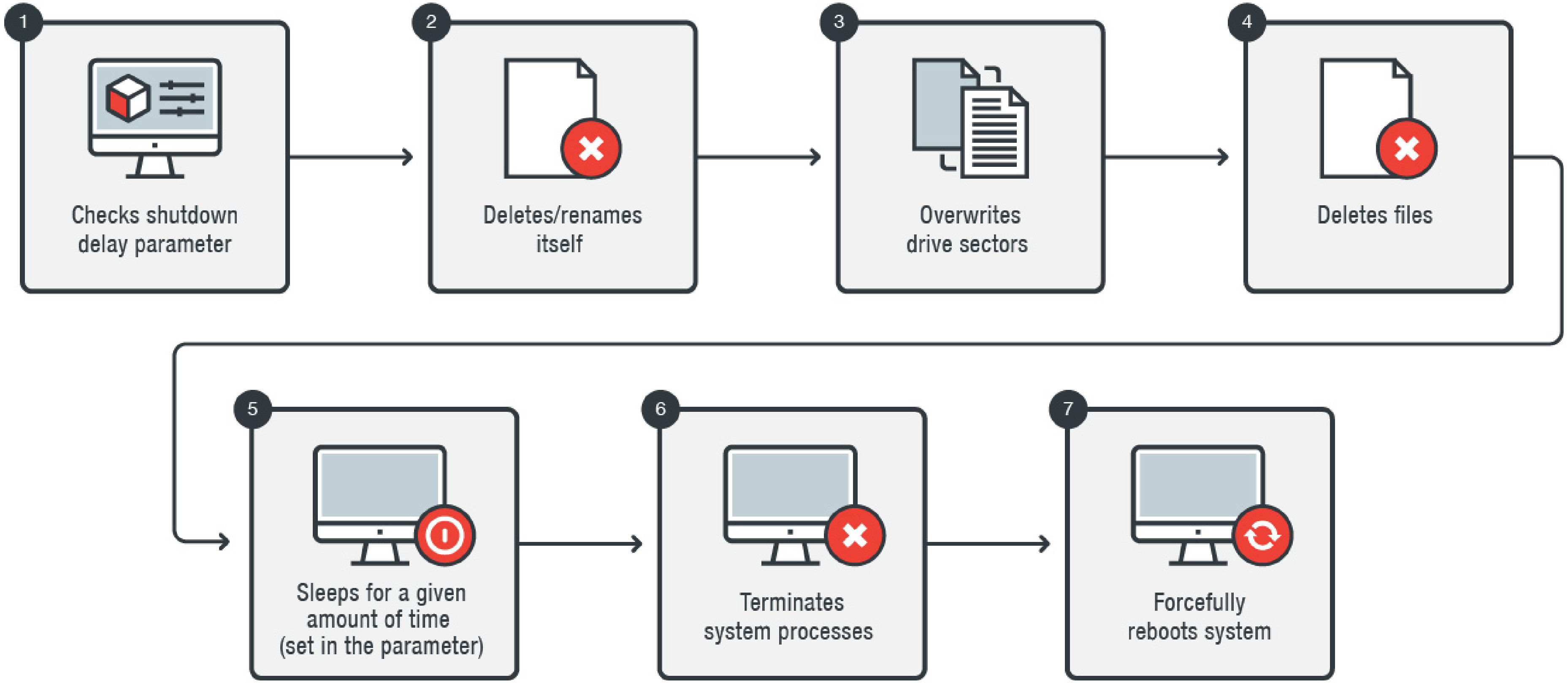
  2014  BlackEnergy 3, Defense mechanisms were implemented:

  - ■ detecting virtual environments
  - ■ anti-debugging methods
  - ■ continuing checks throughout the code that will kill the program if it detects other security functions or countermeasures.

  - ○ This version uses many plug-ins which contributes to making BlackEnergy 3 more user friendly for the hackers
  - ○ *Now 2020 the successor is GreyEnergy*

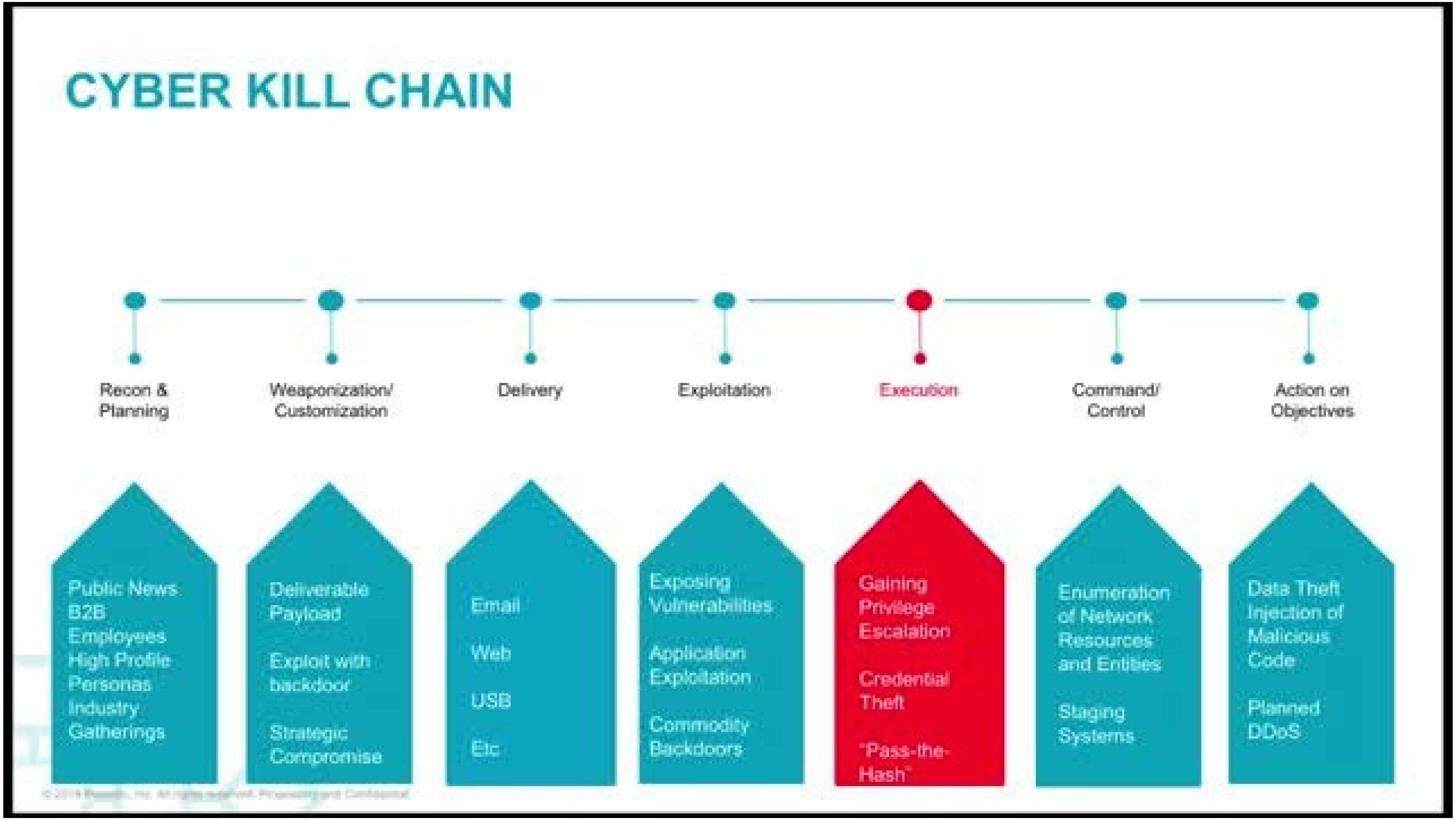
KillDisk destroy harware wipe disks

# KillDisk



1. Checks shutdown delay parameter
2. Deletes/renames itself
3. Overwrites drive sectors
4. Deletes files
5. Sleeps for a given amount of time (set in the parameter)
6. Terminates system processes
7. Forcefully reboots system

# CKC



## CYBER KILL CHAIN

**Recon & Planning**

- Public News
- B2B
- Employees
- High Profile Personas
- Industry Gatherings

**Weaponization/ Customization**

- Deliverable Payload
- Exploit with backdoor
- Strategic Compromise

**Delivery**

- Email
- Web
- USB
- Etc

**Exploitation**

- Exposing Vulnerabilities
- Application Exploitation
- Commodity Backdoors

**Execution**

- Gaining Privilege Escalation
- Credential Theft
- "Pass-the-Hash"

**Command/ Control**

- Enumeration of Network Resources and Entities
- Staging Systems

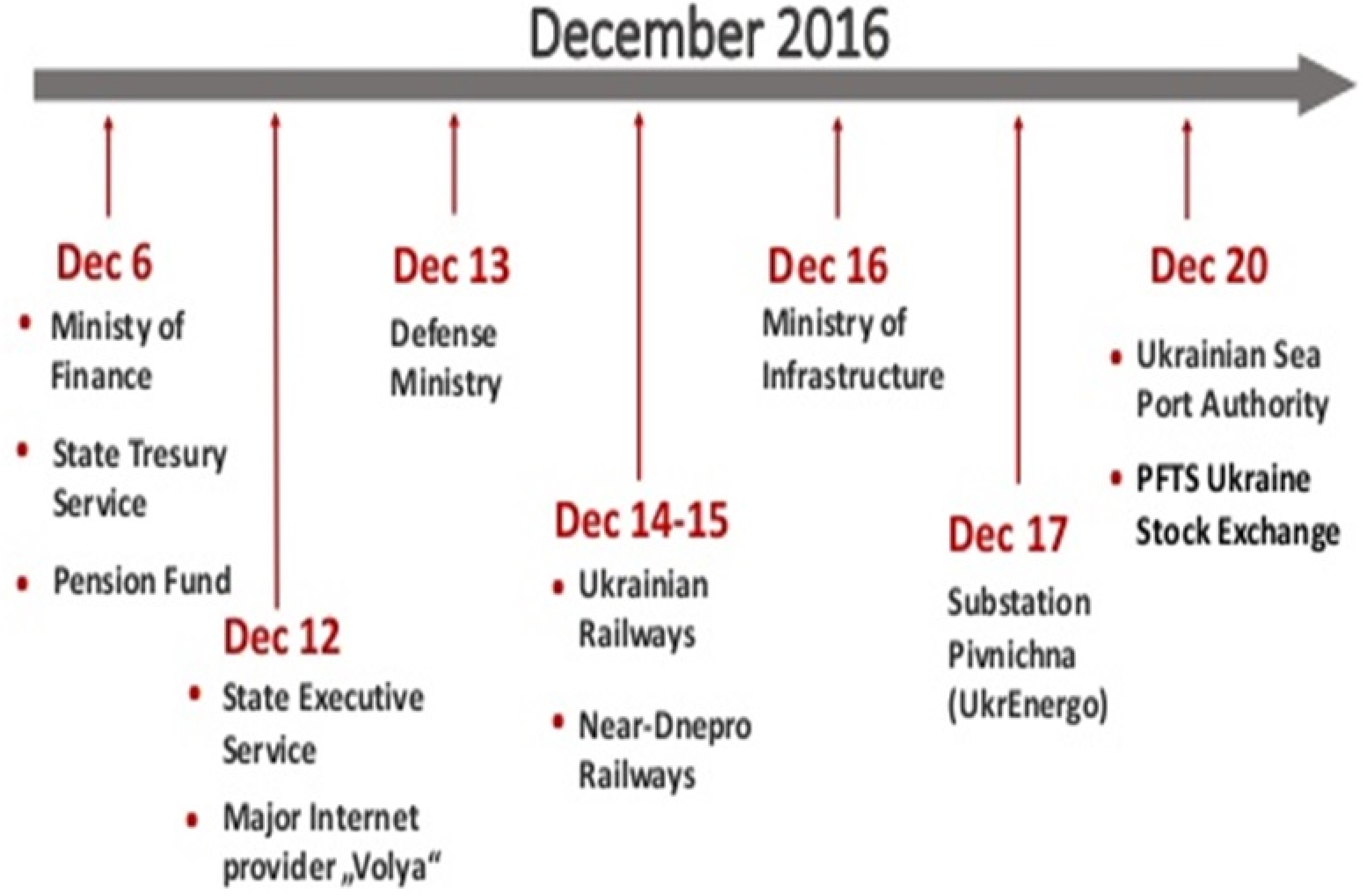
**Action on Objectives**

- Data Theft
- Injection of Malicious Code
- Planned DDoS

# Ukraine Dec 2015 and Dec 2016

- Powergrid blackout by BlackEnergy and KillDisk
  - through hijacked VPNs.
    - They used commands to disable UPS-systems (Uninterruptible Power Supply).
    - Launched  a TDoS-attack, which made the telephone system of customer service unreachable.
    - Planned everything carefully in order to win extra time.
  - After manipulation of the converters, they became unusable.
    - It required physical access in order to replace the software manually.
-

# ~6500 Infrastructure attacks during Dec 2016



December 2016

**Dec 6**

- Ministy of Finance
- State Tresury Service
- Pension Fund

**Dec 12**

- State Executive Service
- Major Internet provider „Volya“

**Dec 13**

Defense Ministry

**Dec 14-15**

- Ukrainian Railways
- Near-Dnepro Railways

**Dec 16**

Ministry of Infrastructure

**Dec 17**

Substation Pivnichna (UkrEnergo)

**Dec 20**

- Ukrainian Sea Port Authority
- PFTS Ukraine Stock Exchange

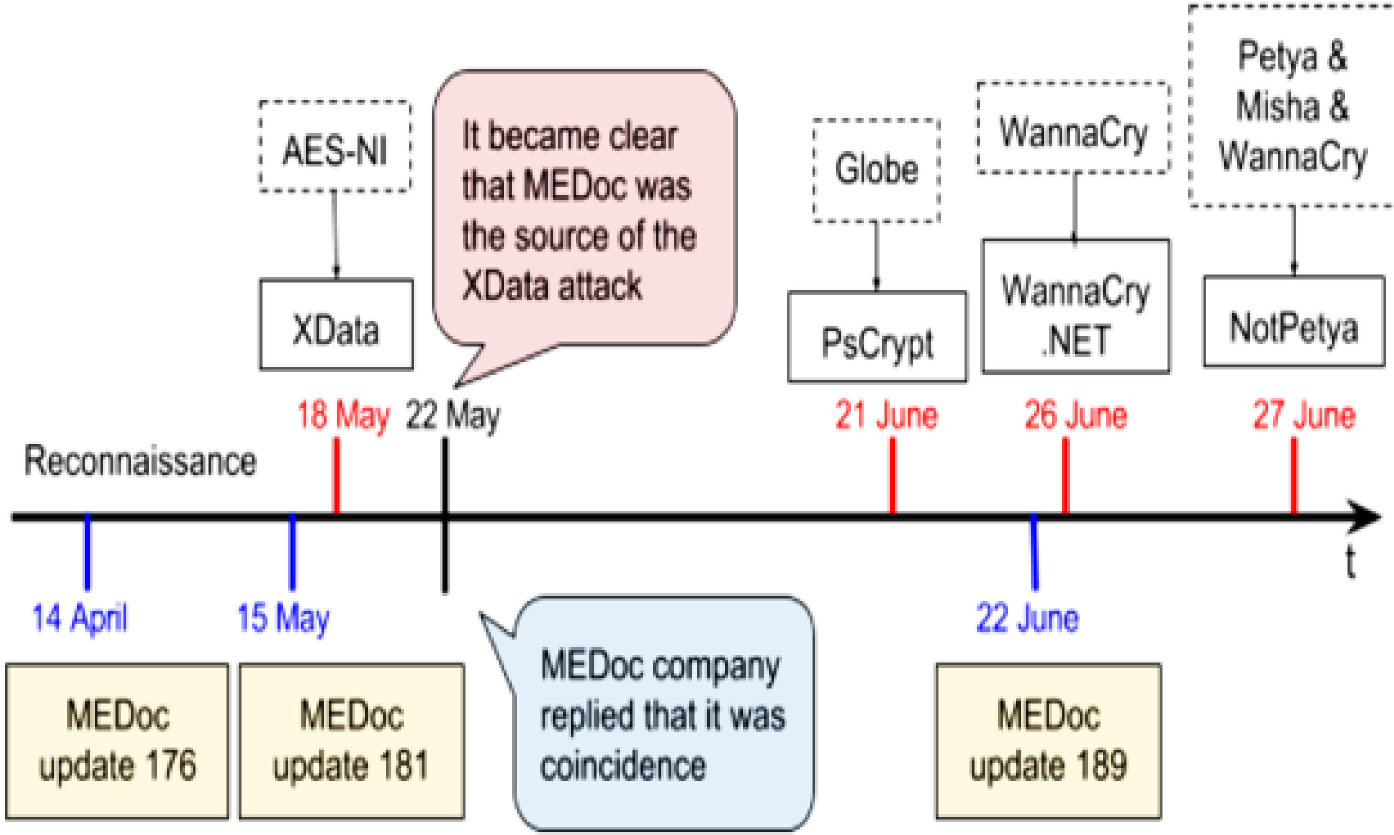
# NotPetya  June 2017

Ukraine, Kharkiv,
local supermarket

19 container ports closed, Gothenburg harbor is one of these
The computer virus NotPetya has hit the freight giant
A.P. Moller-Maersk, and knocked out the company's IT system
~44000 computers
~5000 Servers

# The real story of NotPetya operated by Unit 74455 (GRU)

supply-chain attack through the popular in Ukraine *M.E.Doc* accounting software



* Spy software

in the end it destroyed all infected computer looks like the Petya, . finish with ”Killdisk”

# APT10 and
# Operation Cloud Hopper

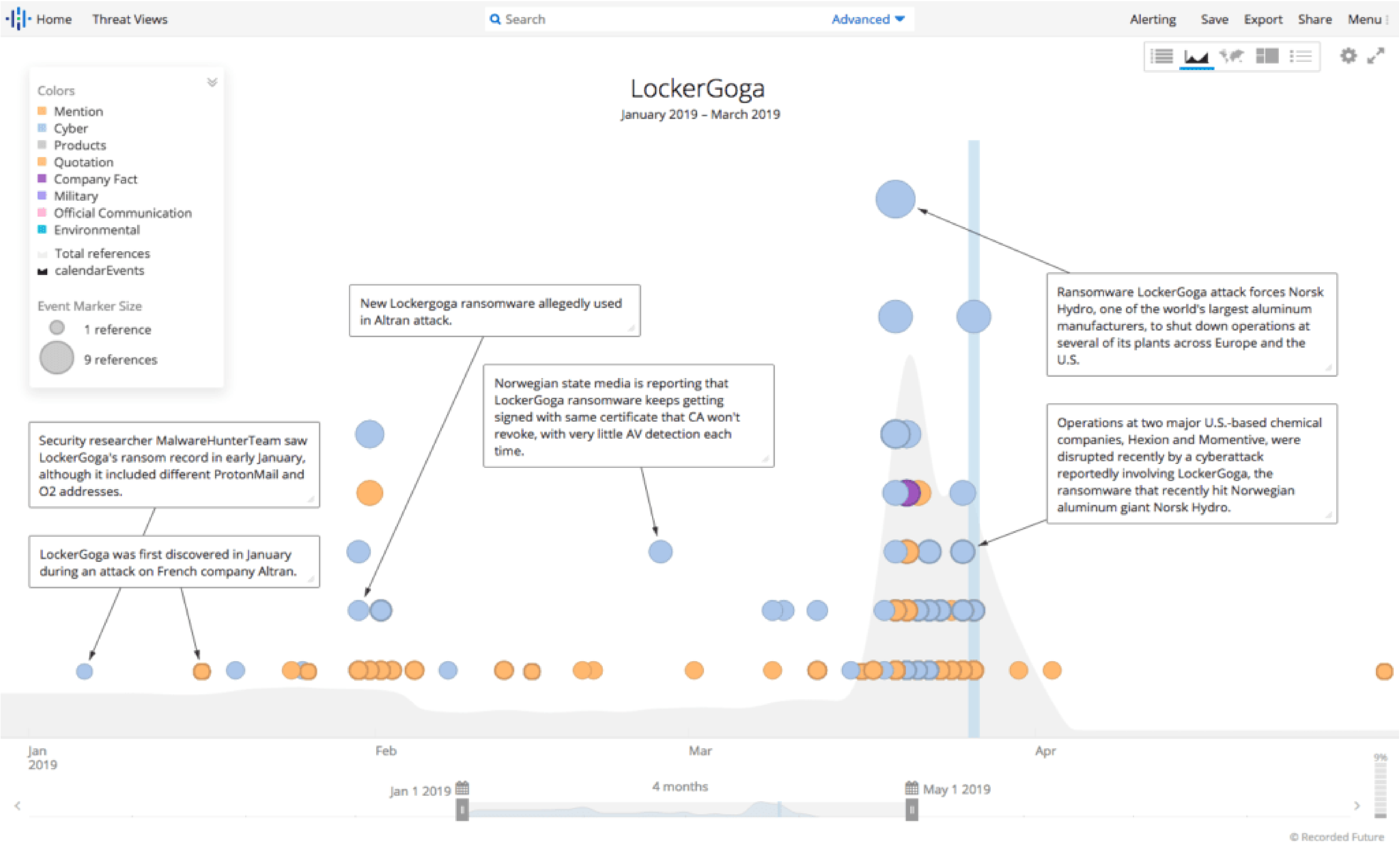
APT10 (a.k.a. MenuPass, POTASSIUM, Stone Panda, Red Apollo, and CVNX)

originate from China

"thought to be one of the largest ever sustained global cyber espionage campaigns in an operation.“

Targeting cloud operator that serv military contractors: BAE, SAAB missile

2017, reemerges in new versions 2018 – 2019 - 2020



## LockerGoga

January 2019 – March 2019

Security researcher MalwareHunterTeam saw LockerGoga's ransom record in early January, although it included different ProtonMail and O2 addresses.

LockerGoga was first discovered in January during an attack on French company Altran.

New Lockergoga ransomware allegedly used in Altran attack.

Norwegian state media is reporting that LockerGoga ransomware keeps getting signed with same certificate that CA won't revoke, with very little AV detection each time.

Ransomware LockerGoga attack forces Norsk Hydro, one of the world's largest aluminum manufacturers, to shut down operations at several of its plants across Europe and the U.S.

Operations at two major U.S.-based chemical companies, Hexion and Momentive, were disrupted recently by a cyberattack reportedly involving LockerGoga, the ransomware that recently hit Norwegian aluminum giant Norsk Hydro.

# 29 April - 5 May 2020 Flooring company Tarkett hit by cyber-attack

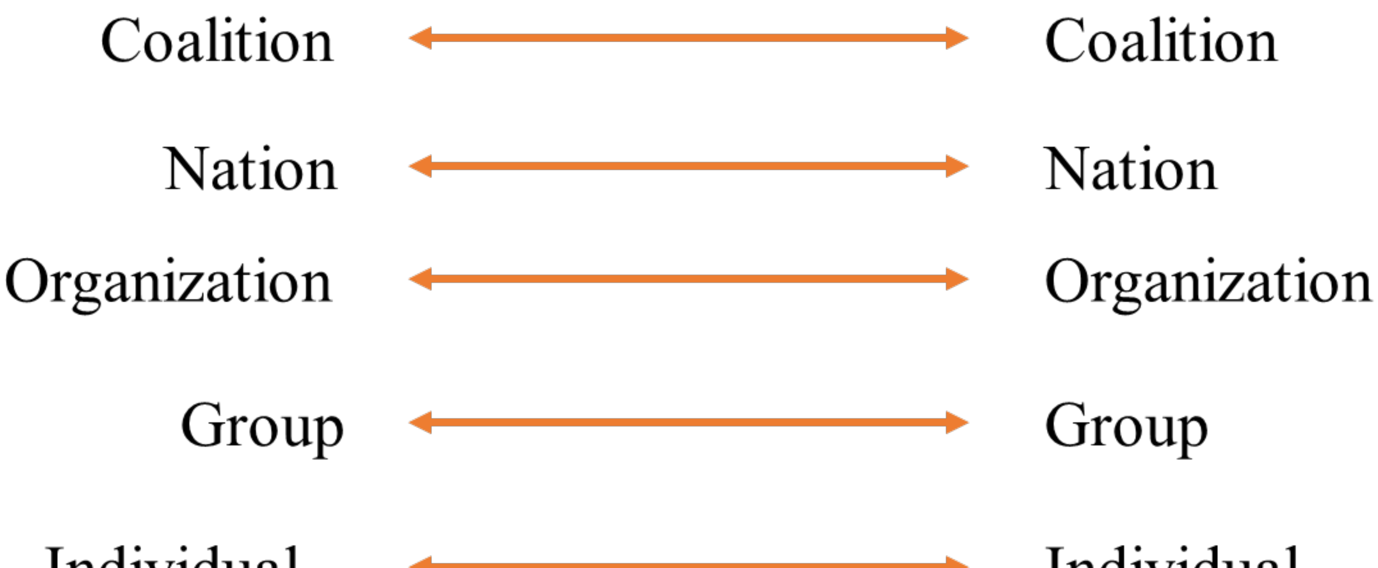
- Hacker group Ragnarok recently stole up to 10TB of data belonging to Portuguese energy giant EDP and is now threatening to leak the stolen data if a ransom of $10.9 million is not paid by the company.

- Iranian hackers stole terabytes of data, Dec. 2018 and again on March 4th 2019.

  They made off with at least 6TB of documents and as much as 10TB from service provider CITRIX, focused on project data for the Aerospace industry, the FBI, NASA and Saudi Arabia's state-owned oil company.

- https://www.itgovernance.co.uk/blog/list-of-data-breaches-cyber-attacks-may-2020

# Actors then ......



Coalition ↔ Coalition

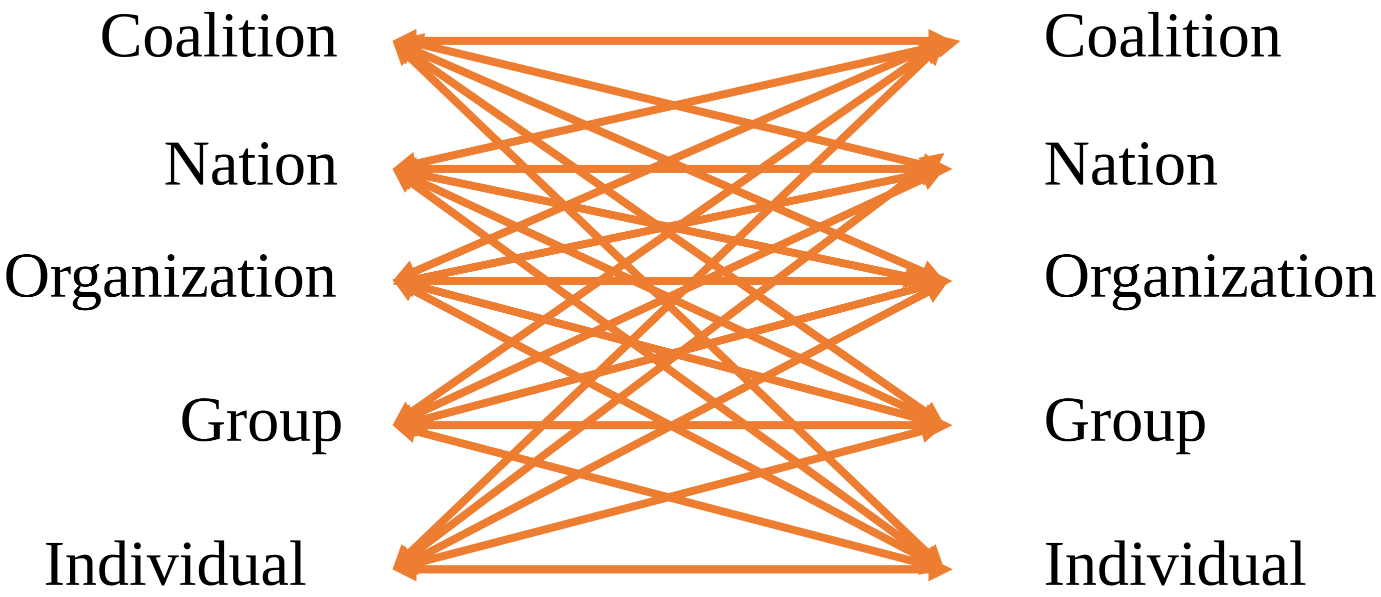
Nation ↔ Nation

Organization ↔ Organization

Group ↔ Group

Individual ↔ Individual

# Actors Now !!!



Coalition

Nation

Organization

Group

Individual

Coalition

Nation

Organization

Group

Individual

# APT 39 a.k.a ”ChaferAPT”, ”RemixKitten”

- Is a Iranian cyber espionage targeting Turkish, Kuwait, SaudiArabia and telecommunication & travlerer industry in the Middel East collecting personal information that serv geoplolitical intrests.

# Motivations and Consequences for State-sponsored cyberattacks

- Customer data, Intellectual Property lost of trade secrets, harvesting corporate data can be devastating.

- Quick step to launch new plants and productions units from stolen research and product information.

- Intercepted market plans used by unscupulous cometitors.

- Hostile takover, using stockmarket

- Iran has been charge with stealing 3.4 billion scientific data from 8000 Professors at 3200 universities (2018).
- US economy estimate lost of $600 billion annualy for stole trade secrets.

https://www.radware.com/documents/infographics/intellectual-property-cost-infographic

- https://www.youtube.com/watch?v=btZhrmK2sYA

Does this sound interesting?

# PROMIS (Professional Master in Information Security)

GENERAL FORMAT

**Active industrials studying and working at the same time**

- *University grade **COURSES for professionals**!*
- *Extend current competence in **an area ("security")***
- Case-based pedagogy (bring your own problems!)
- On-line collaborative didactics
- Distance capability overall incl. lab and tools

**Courses under development with input from companies**

- Keep relevant and right level (companies advise us)
- DO YOU want to be part of the companies advising on courses?
  - CONTACT: Anna Eriksson aes@bth.se

BALLOU
VI ÄR EXPERTER PÅ DRIFT - ÄR NI?
citynetwork
ERICSSON
CYBERCOM GROUP
Outpost24
PROMESTRA
telenor
TRUESEC
advenica
factor10
MaxKompetens
HELP AT WORK

*more to come*

# Courses (3 thus far)

**PROMIS** (Professional Master in Information Security)

https://promisedu.se/

**Security in Software-intensive products and service development** (PA2582)
https://www.bth.se/eng/courses/D5818/20202/
Course responsible: Tony Gorschek tony.gorschek@bth.se

- The ability to understand the technology, operational aspects, and engineering aspects of security - albeit the focus on the course is on "engineering security”
- The ability to plan for "pre-emptive" security in the planning and development of products and services
- The ability to do a risk assessment and take ROI into account
- The ability to develop and use secure architectures that allows for a more stable base for products and services
- The ability to compare and weigh the benefits and costs of non-functional aspects in combination to security
- The ability to estimate how security aspects impact, and are impacted on quality-/non-functional aspects such as usability, performance and maintainability of a product

*more to come*

# Courses (3 thus far)

**PROMIS** (Professional Master in Information Security)

https://promisedu.se/

**Software Security** (DV2595)
https://www.bth.se/eng/courses/D5816/20202/
Course responsible: Dragos Ilie dragos.ilie@bth.se

- The ability to  understand how attackers exploit risky programming practices
- The ability to detect risky programming practices
- The ability to understand and reason about efficiency and limitations in existing software security mechanisms
- The ability to to compare and weight the benefits and costs associated with binary analysis and instrumentation techniques

*more to come*

# Courses (3 thus far)

**PROMIS** (Professional Master in Information Security)

https://promisedu.se/

**Web System Security** (DV2596)
https://www.bth.se/eng/courses/D5816/20202/
Course responsible: Anders Carlsson anders.carlsson@bth.se

- be able to explain web protocols based on known vulnerabilities and weaknesses
- be able to describe the Common Vulnerability Scoring System (CVSS)
- be able to explain web protocols based on known vulnerabilities and weaknesses
- be able to explain the security aspects when using languages and framework, eg. PHP, JavaScript, and SQL
- be able to explain authentication mechanisms and counter techniques to bypass authentication
- understand Cross-site scripting (XSS) attacks and SQL injections
- be able to explain impacts of one or more combined vulnerabilities that limit or extend the damage given
- be able to install and configure the web server for high security independently
- be able to use and search open vulnerability databases (Common Vulnerability databases CV -DB) to prevent and find security problems
- be able to use best practice of known design patterns for secure web applications
- be able to utilize OWASP where applicable
- be able to conduct internal and external penetration testing of web applications and related infrastructure)

*more to come*

# PROMIS

## HOW TO APPLY

https://promisedu.se/

**Spread information about courses @ your company**

**Entry Requirements**

*PROMIS courses requires at least 120 credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).*

Even if you don't have the formal academic merits, you might be qualified for the course through validation (reell kompetens)!

**Apply for course:**

1. **Create a user account at antagning.se / universityadmission.se**
2. **Search for PROMIS courses by the name Fill in and send in your application**
3. **Upload your required documents (employer's certificate)**
4. **Reply to any offers of admission**

**Questions about the course:** contact course responsible
**Questions about applying and validation (reell kompetens): :** anna.eriksson@bth.se
Visit promisedu.se for more info about courses, application and template for employer's certificate