



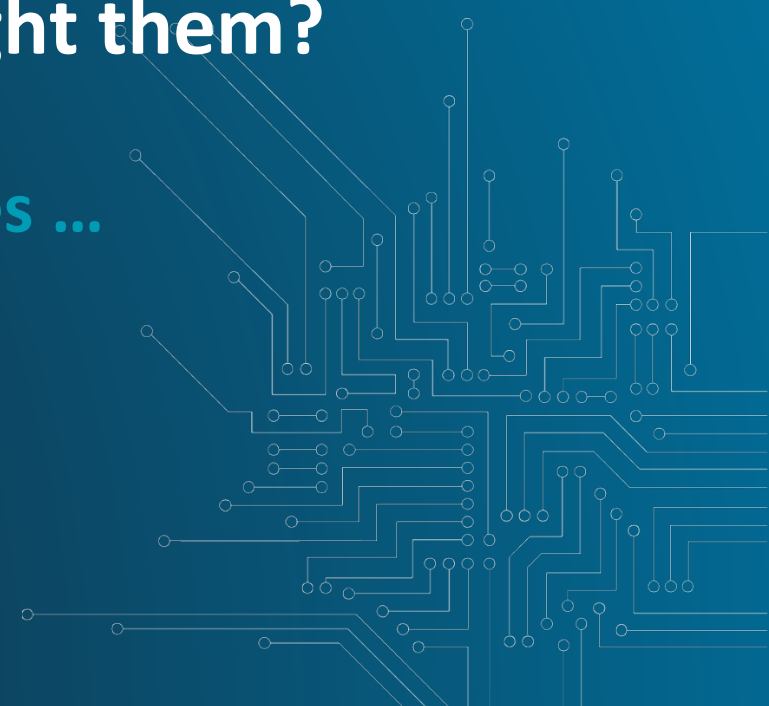
CENTRE FOR
CYBER SECURITY
BELGIUM

The security perspective : what are the cyberthreats and how to fight them?

Cloud Computing : opportunities ... and threats ! 25/02/2019

Phédra Clouner

Deputy Director



01

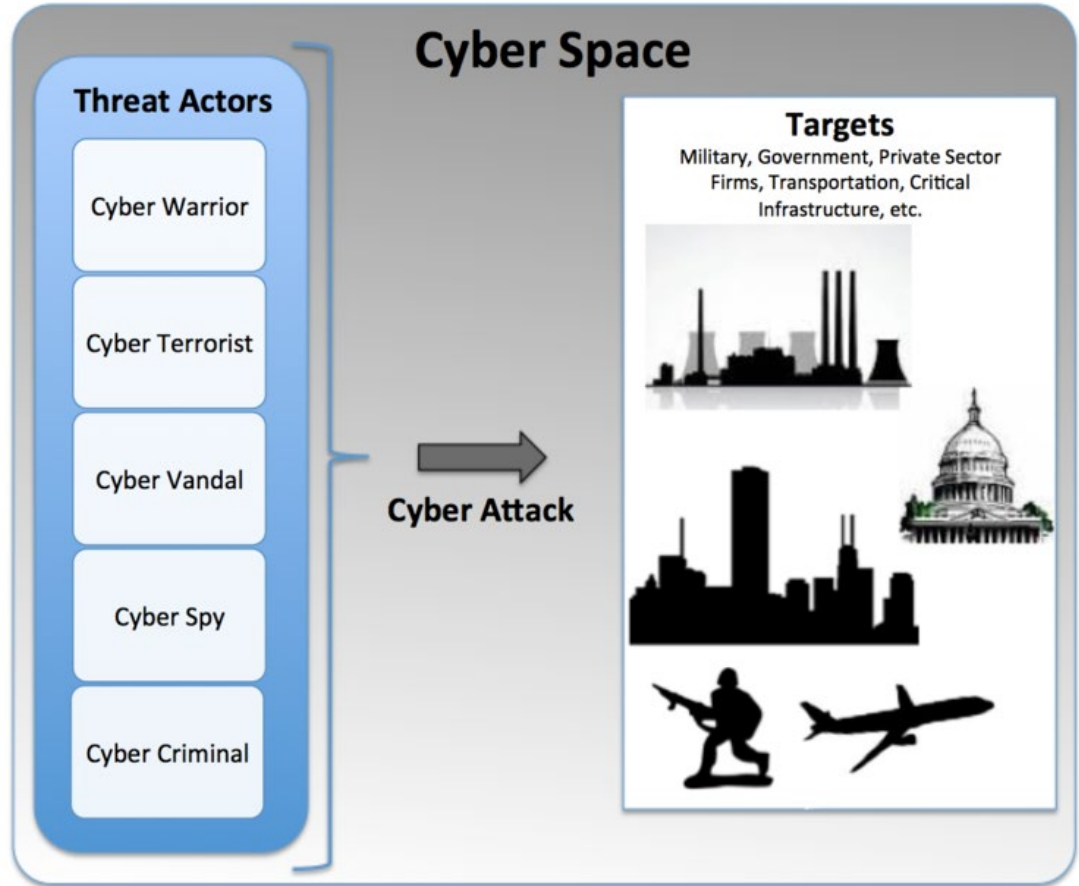
What kind of Cyberthreat?















































There are only two
types of companies,
those who got hacked
and those who will be.




Robert Mueller

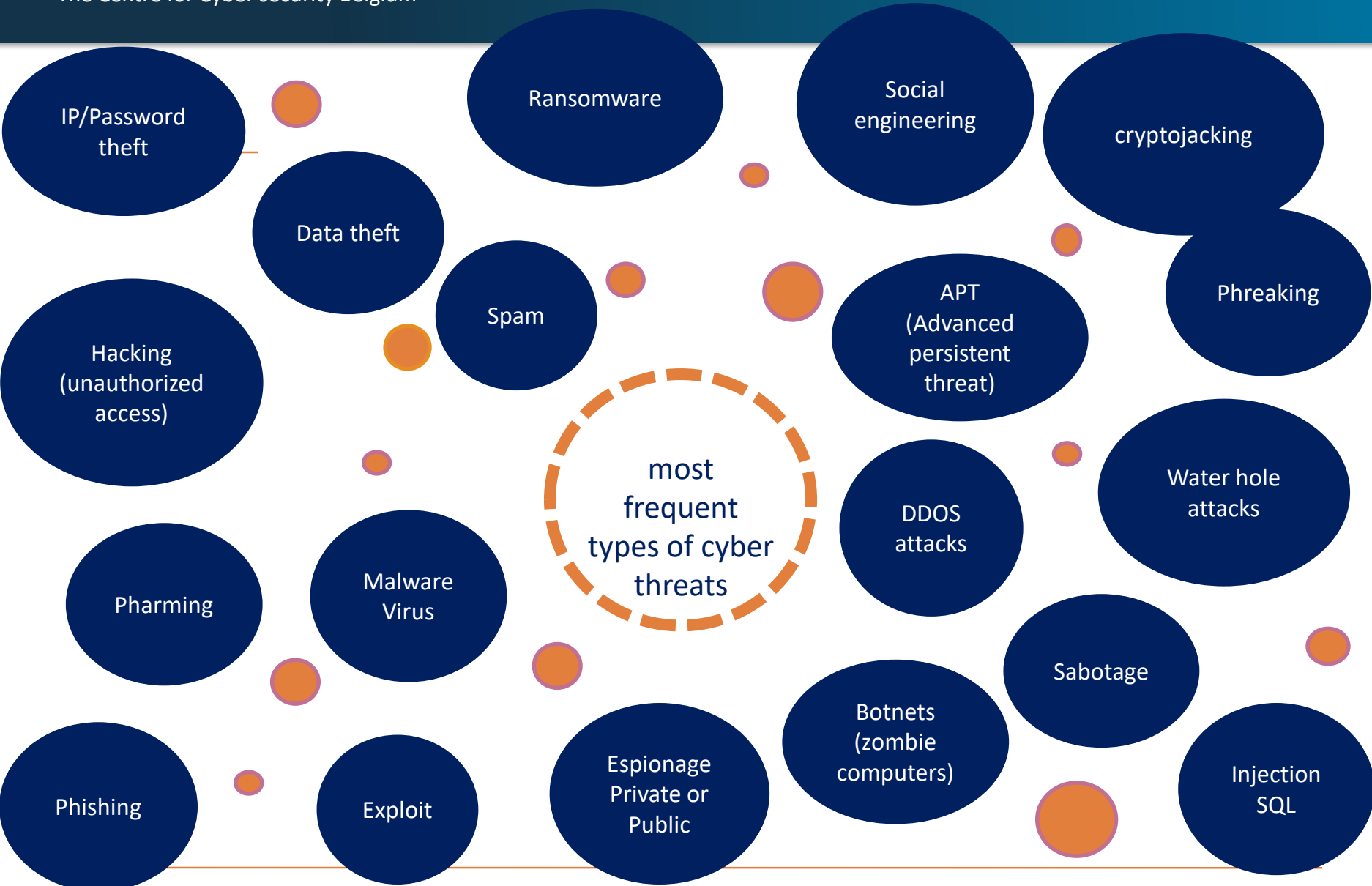
THREAT ACTORS



Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware		1. Malware		
2. Web Based Attacks		2. Web Based Attacks		
3. Web Application Attacks		3. Web Application Attacks		
4. Phishing		4. Phishing		
5. Spam		5. Denial of Service		
6. Denial of Service		6. Spam		
7. Ransomware		7. Botnets		
8. Botnets		8. Data Breaches		
9. Insider threat		9. Insider Threat		
10. Physical manipulation/ damage/ theft/loss		10. Physical manipulation/ damage/ theft/loss		
11. Data Breaches		11. Information Leakage		
12. Identity Theft		12. Identity Theft		
13. Information Leakage		13. Cryptojacking		NEW
14. Exploit Kits		14. Ransomware		
15. Cyber Espionage		15. Cyber Espionage		



Legend: Trends:  Declining,  Stable,  Increasing



Threats for companies

- Industrial Spying
- Theft €
 - CEO Fraude
- Extortion
 - DDOS
 - Ransomware
 - *Informatie theft*
- Disturbance



Risk Analysis

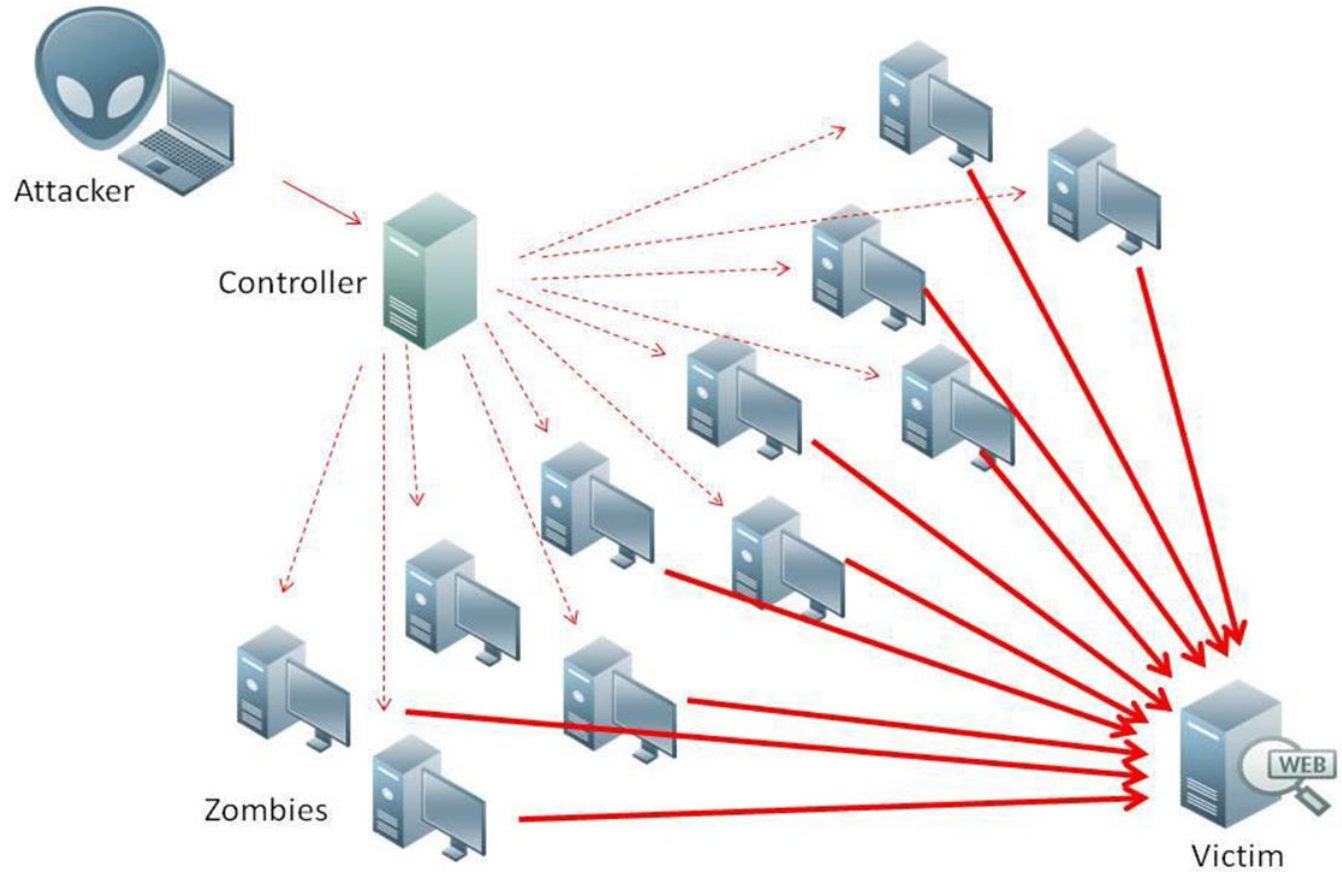
- Outsider threat
- Insider threat: rogue employee
- Insider threat: negligence
- Technical failure
- Calamities

Protect



DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

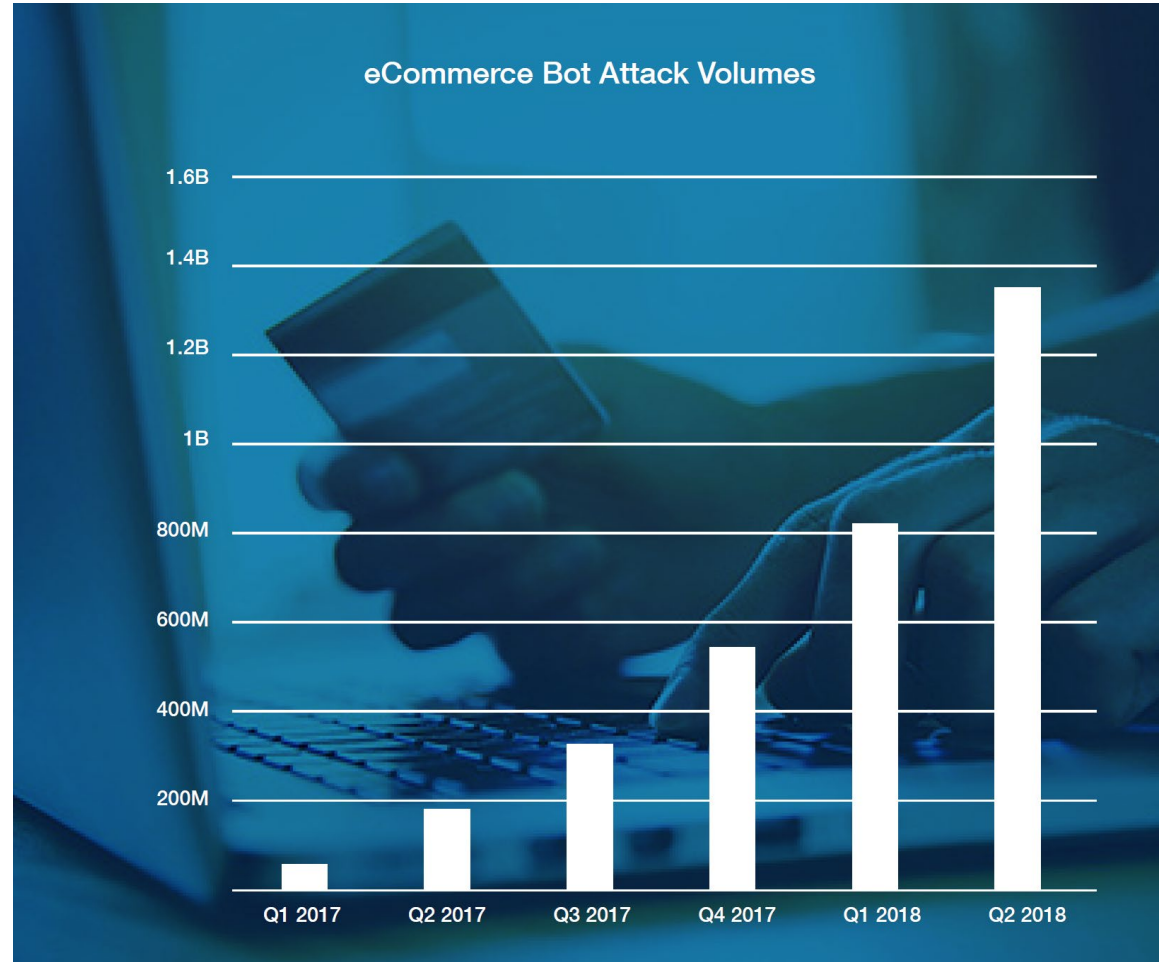
BOTNETS



Pumping up the volume

70 Mio
mobile

IoT
powerful attacks
that could severely
disrupt the
Internet



DDOS

Survey Peak Attack Size Year Over Year

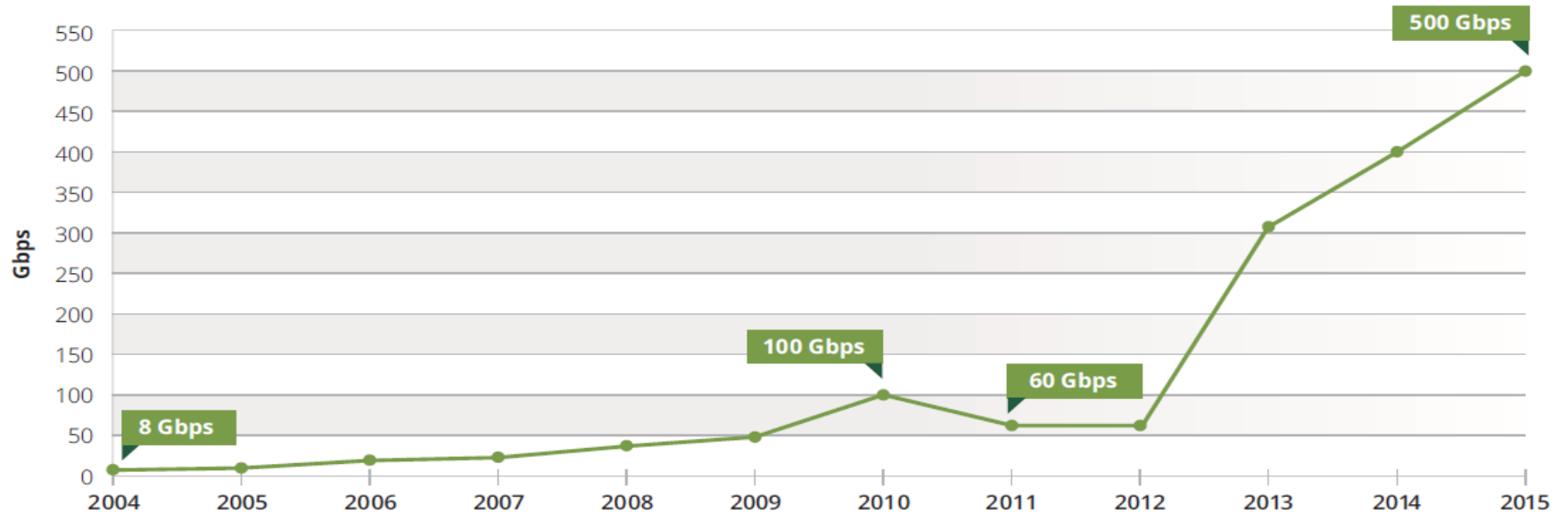


Figure 14 Source: Arbor Networks, Inc.

- Strong increase volumes through botnets of internet-connected devices
- The Internet of Things (IoT)

Threat @ home

Social
engineering

Phishing

Ransomware

Information
Theft



Ransomware – Cryptoware (Remember the WannaCry — Ransomware 12-15/5/2017)

CryptoLocker



Private key will be destroyed on
1/6/2015 1:11:47 PM

Time left
71:52:21

Checking wallet..
Received: **0.00 BTC**

Your Personal files are encrypted!

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **1.00 bitcoin** (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not move your files.

[Show files](#) [Pay with Bitcoin](#)

What is an APT?



APT

Features of an APT

- Complex malware.
- Difficult to detect – traditional protection (Firewall, Anti-Virus, IDS ...) is inadequate.
 - IT - Stealth technology
 - Can attack different types of operating systems. (Incl Scada, Solaris, Linux, Router OS, **MOBILE** ...)
- Often “a la carte” developed for one specific victim or a small group of victims.
 - General IOCs are insufficient
- Controlled by a team of people who have considerable resources.
 - Often state-sponsored.

Features of an APT

Persistent

- An APT is developed to stay under the radar as long as possible. Sometimes it takes years before an intrusion is discovered..
 - IT - Stealth technology
- If a cleanup is performed, it often happens that the system is reinfected within a few hours / days.
- **Threat:**
 - Data exfiltration
 - Sabotage

Goal of an APT

- State sponsored espionage (intelligence services)
 - Data exfiltration
 - Victim's observation.
 - Building backdoors into products.
 - Provide a permanent presence ...



Goal of an APT

- Economic-Scientific espionage
 - State-Sponsored (o.a. 1 dossier in Oost-Vlaanderen)
 - Criminal organisation



Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets



Goal of an APT

- Financial gain:

- Criminal organizations

- National bank Bangladesh / Swift (+/- 100 miljoen \$\$\$)
- Carbanak case (1 miljard \$\$\$)
-

- Ex-Gov staff /Criminal organizations

- Malware-as-a-Service
- Access-as-a-Service
- APT-as-a-Service
-

- Disruption of a state:

- Wada hack by Fancy Bears
 - Clinton mails / DNC Hack
 - Influence on election (cfr. US)
 -
-

Goal of an APT

- Cyber Warfare
 - Cyber Sabotage & Spionage
 - Offensive / Defensive
 - SGRS (Mil BE)



Goal of an APT

- **Cyber Terrorisme**
 - Terro groups
 - Sabotage (Utilities, transport, financial sector, ...)
 - Financing of terro (cfr. Carbanak, Bangladesh, ...)
 - Quid current possibilities / expertise?



- Malware-as-a-Service
- Access-as-a-Service
- APT-as-a-Service

The complexity of an APT

- The life cycle / kill chain of an APT

How the Carbanak cybergang stole \$1bn A targeted attack on a bank

1. Infection



100s of machines infected in search of the admin PC



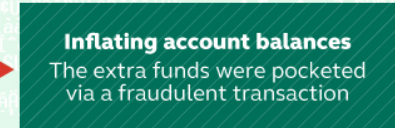
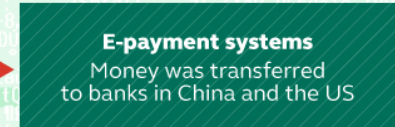
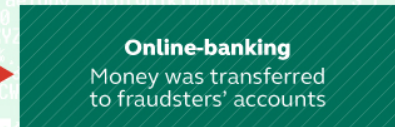
2. Harvesting Intelligence

Intercepting the clerks' screens



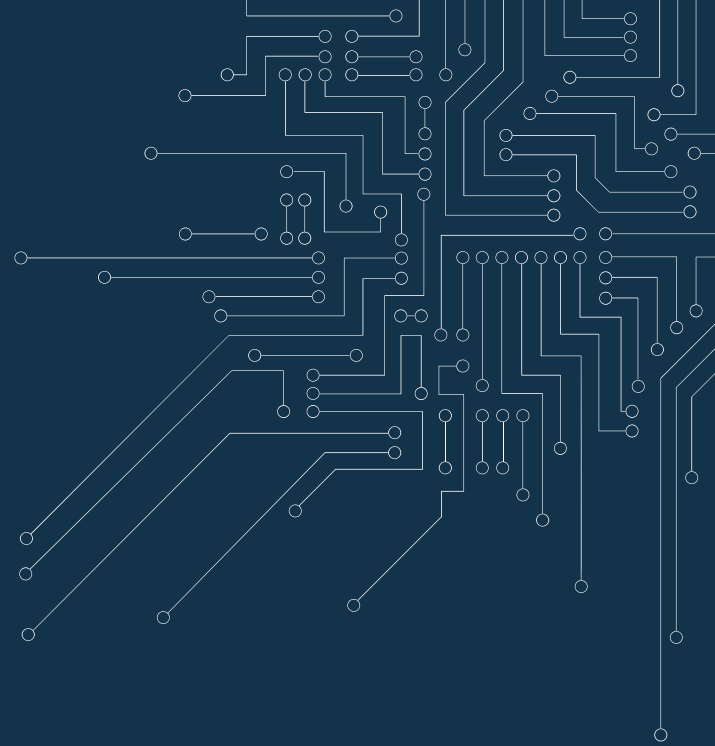
3. Mimicking the staff

How the money was stolen

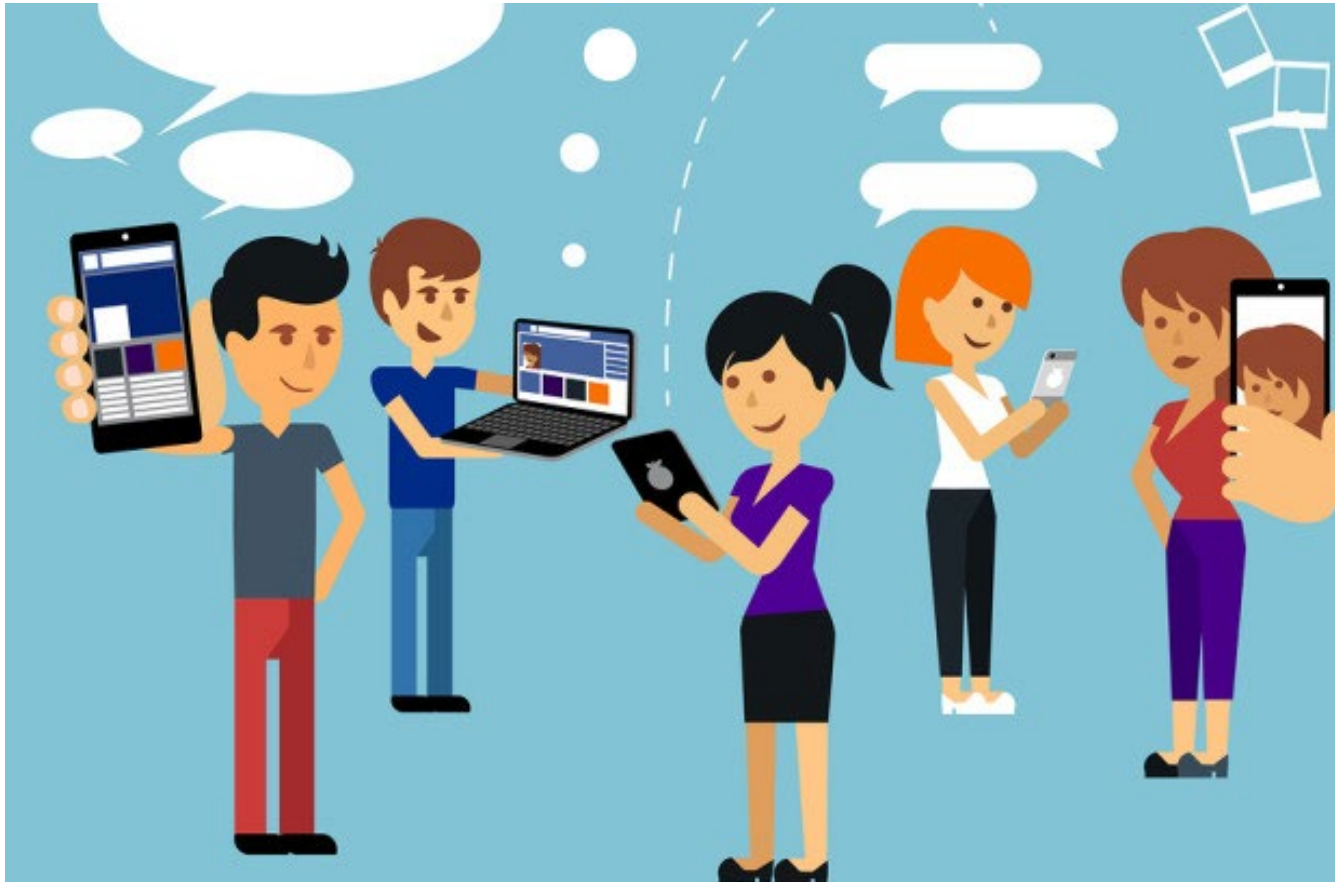


02

How to protect?



Protect ALL your devices AND yourself !!



SafeOnWeb Recommendations

1. Scan your computer and use an antivirus software
2. Keep your program's up-to-date
3. Make back-ups (cloud)
4. Recognise phishing
5. Use strong password

Safeonweb.be

FAITES LE **Test du phishing**
Identifiez-vous à temps les messages suspects ?

1 MESSAGE NON LU

AUJOURD'HUI

250 euros à gagner chez Delhaize via WhatsApp : Rendez-vous sur : <http://delhaize-be.site> des bons d'une valeur de 250 € offerts par Delhaize. Delhaize fête son anniversaire. Je pense que cette offre est limitée. J'en ai déjà profité. ❤️ 13:17

Message promotionnel Delhaize via WhatsApp

Question 1/6

Qu'y a-t-il de suspect dans ce message WhatsApp ?

- La date et l'heure du message.
- Le lien renvoyant au site web (<http://delhaize-be.site>).
- Une campagne promotionnelle pour l'anniversaire de Delhaize.
- Delhaize envoie ce message promotionnel via WhatsApp.
- Un cœur est reproduit à la fin du message.
- La promotion est trop belle pour être vraie.

Vérification

Safeonweb.be

Safeonweb.be a pour ambition d'informer rapidement et efficacement les citoyens belges en matière de sécurité informatique, des plus récentes et plus importantes menaces.

Recognise phishing

- Unsubscribed/ unknown email address or not from a known organization (by ex: Anne58632@gmail.com)
- You get scared and have to take action quickly
 - Something wrong with your bank account
 - An expensive order that you never placed
- Your name is not used in the message
- The message contains writing errors or an unnatural language
- You will be asked to submit online personal information
- Attachment or link
- Link does not match what can be expected.
- Your system requests unexpected permission to install a program.

→ AWARENESS IS ONE OF THE KEYS!



Campagne 2018 – Update & Backup

Van een back-up word je zen



Boost je digitale gezondheid.

MAAK BACK-UPS VAN JE GEGEVENS OP COMPUTER, SMARTPHONE EN TABLET VOOR HET TE LAAT IS. MEER TIPS OP SAFEONWEB.BE.

Regelmatige updates maken je gezonder



Boost je digitale gezondheid.

UPDATE NU JE COMPUTER, SMARTPHONE EN TABLET VOOR HET TE LAAT IS. MEER TIPS OP SAFEONWEB.BE.

Cyber Security Reference Guide



CENTRE FOR
CYBER SECURITY
BELGIUM

Search



Plan your cyber security

Define your strategy and your security politics.

[READ MORE](#)



Manage risks for your most important assets

Identify your important assets and the risks they run.

[READ MORE](#)



Take security measures

Implement your security measures.

[READ MORE](#)



Evaluate your actions

Continually evaluate your results.

[READ MORE](#)



CENTRE FOR
CYBER SECURITY
BELGIUM

Cyber Security Reference Guide

Take security measures / Manage access to your computers and networks

Basic

Advanced

Plan your cyber security

Manage risks for your most important assets

Take security measures

Have a business continuity and an incident handling plan

Manage access to your computers and networks

Manage your key ICT assets

Install antivirus protection

Update all programs

Back up all information

Secure remote access

Secure workstations and mobile devices

Secure servers and network components

Secure your website

Evaluate your actions

MANAGE ACCESS TO YOUR COMPUTERS AND NETWORKS

Just as you manage the physical security of your organization, you must manage information security. Do not leave your information accessible to everybody, at any time.

Users are only authorized to access the information they need to perform their duties

Immediately disable unused accounts

Rights and privileges are managed by user groups

Change all default passwords

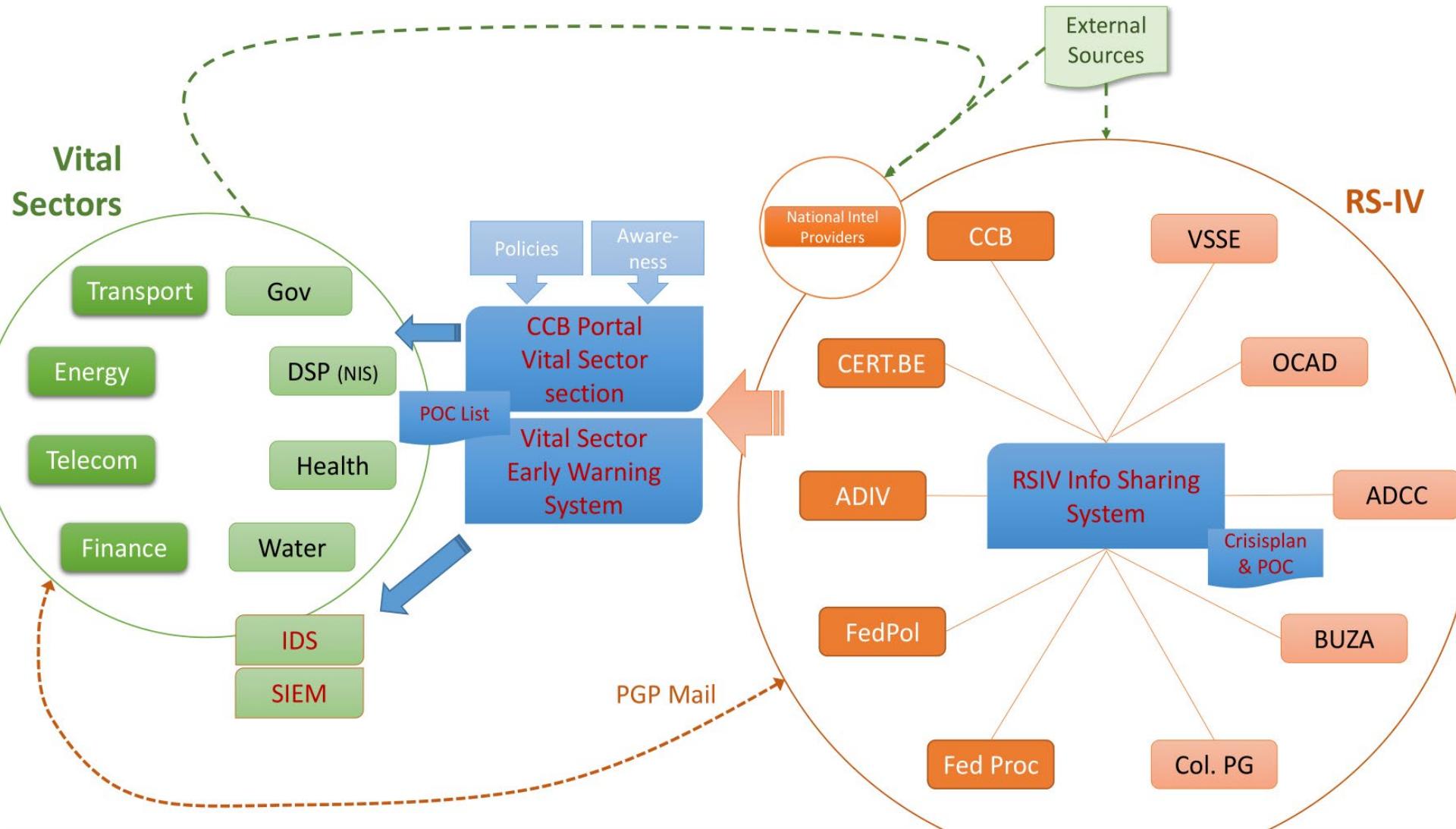
Passwords must be longer than 10 characters with a combination of character types and changed periodically or when there is any suspicion of compromise

Enforce authentication and password rules

Use only individual accounts and never share passwords

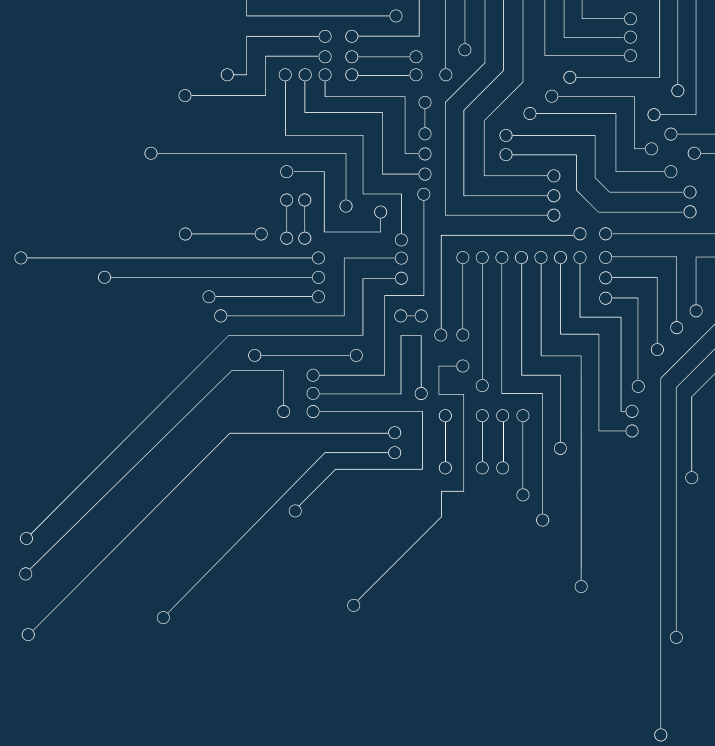
Keep a limited and updated list of system administrator accounts

No one works with administrator privileges for daily tasks



02.1

CCB mission & services



Legal basis

1. Monitoring, coordinating and supervising **the implementation of Belgian policy** on the subject;
2. Managing the various projects on the topic of cybersecurity using an **integrated and centralized approach**;
3. **Ensuring coordination** between the relevant government departments and governments, as well as the public authorities and the private or scientific sectors;
4. Formulating proposals aimed at **adapting the regulatory framework** in the field of cybersecurity;
5. **Ensuring crisis management** in case of cyber incidents in cooperation with the government's Coordination and Crisis Centre;
6. Preparing, disseminating and supervising the **implementation of standards, guidelines and security standards** for the various information systems of the governments and public institutions;
7. **Coordinating the Belgian representation in international cybersecurity forums**, coordinating the monitoring of international commitments and national proposals on this subject;
8. Coordinating the **security evaluation** and **certification** of information and communication systems;
9. **Informing and raising awareness** among users on information and communication systems.

Integration of the Computer Emergency Response team(Cert.be): new organisation (focus: incident handling- information sharing), more capabilities (24 FTE) – High level technical experts

STRATEGIC OBJECTIVES

@home

- Awareness
- Botnet Eradication
- Anti-phishing
- www.safeonweb.be

@work

- Cyber Security guides
- Webinars
- Training (Gov only)
- Partnerships
- Reliable technologies

STRATEGIC OBJECTIVES

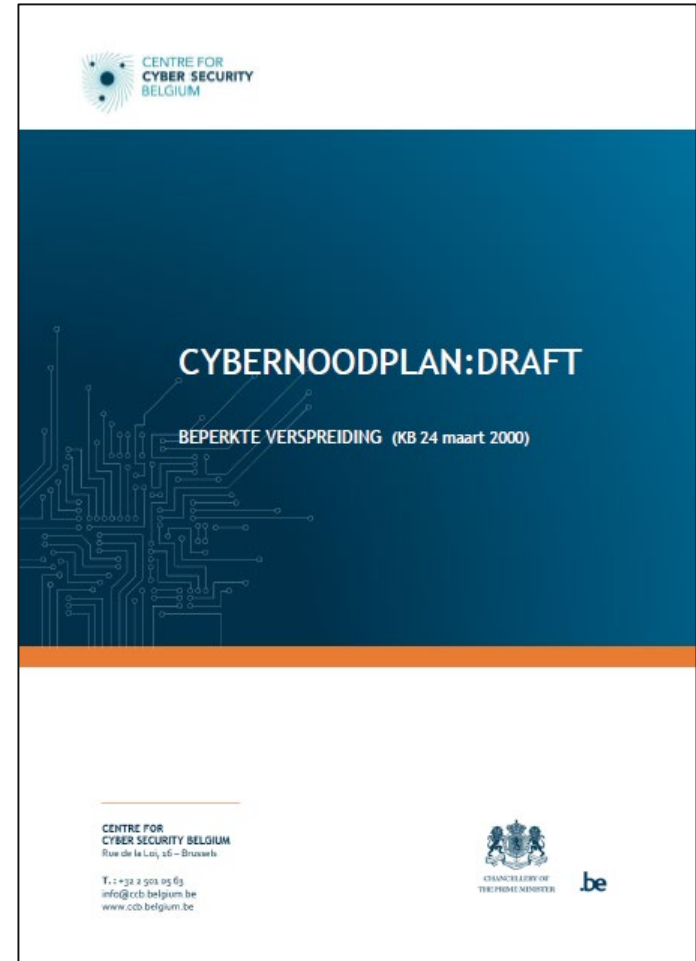
Vital Sectors

Critical infrastructure, government ...

- Early warning-system
 - Threats, vulnerabilities, incidents ...
- Detection & monitoring
 - MISP – Standard IDS - SIEM
- Baseline security norm & audit
 - Directives, guidelines, norms
- Incident response
 - Diagnosis, response
 - Incident management system

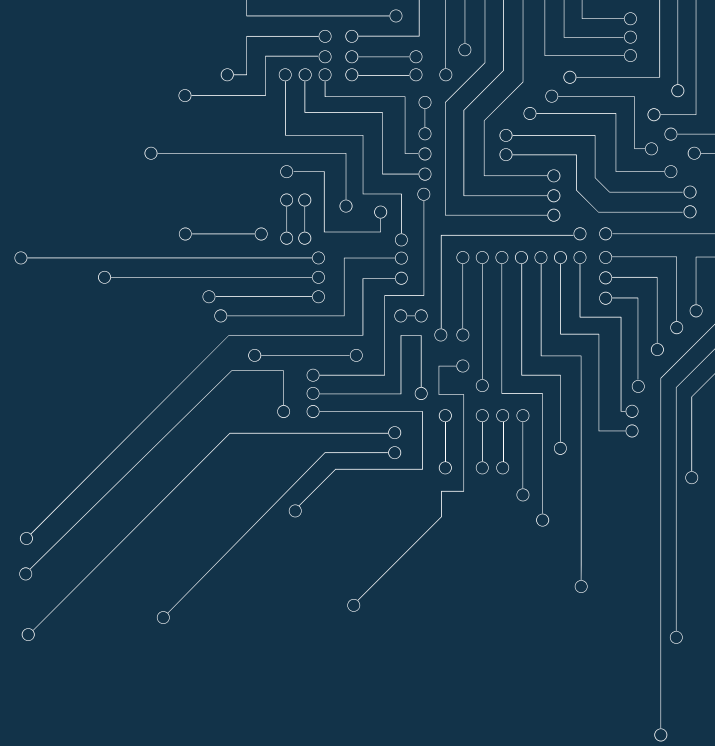
NATIONAL CYBER SECURITY EMERGENCY PLAN

- Upscaling
- Definition of responsibilities
- Procedures
- Tested during exercises
 - (CMX/Cyber Europe 2016)



03

Cybersecurity Incident?



TOWARDS A STRONGER CERT.BE

- Better CERT.BE – CCB collaboration/integration
- More capabilities (24 FTE) – High level technical experts
- > 60 % information sharing
- Incident handling
 - CERT@CERT.BE

Know-how

Trust

CERT.BE 2017

- **Cyber Security Information Sharing**
 - Collect incoming information
 - Collect open source, partner & commercial IOCs and rules
 - Information analysis & registration (quality control, correlation and linkage...)
 - Distribute of advisories & warnings
 - Participate in cyber threat information sharing communities
 - Threat assessment reporting (constituents, management, partners, ...)
 - Register & evaluate incoming messages (assessment, triage, prioritization)
 - Monitor detection tool alerts for Gov sites
 - Trigger necessary actions based on the message evaluation

CERT.BE 2017

- **Incident Response & Intrusion detection**
 - Coordinate incident response (24/7 on call at home)
 - Design the IDS platforms
 - Design architecture to search through logs with SIEM
 - Digital Forensics & artefact analysis
 - (malware analysis, sandboxing...)
 - Creation and distribution of IOCs and rules
 - Vulnerability and penetration testing (on demand)
 - Development and maintenance of systems for handling automated feeds



QUESTIONS ?

