Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

Reporting and Analysis Centre for Information Assurance MELANI

MELANI

Cybersecurity in Critical? Infrastructure

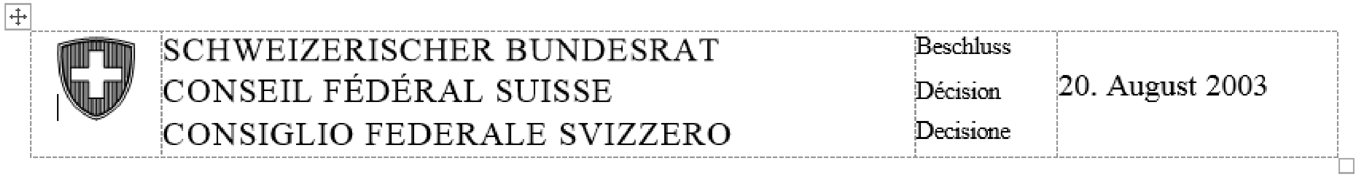
Daniel Rudin, Sector Advisor ICS MELANI / GovCERT.ch

13. October 2016

Agenda

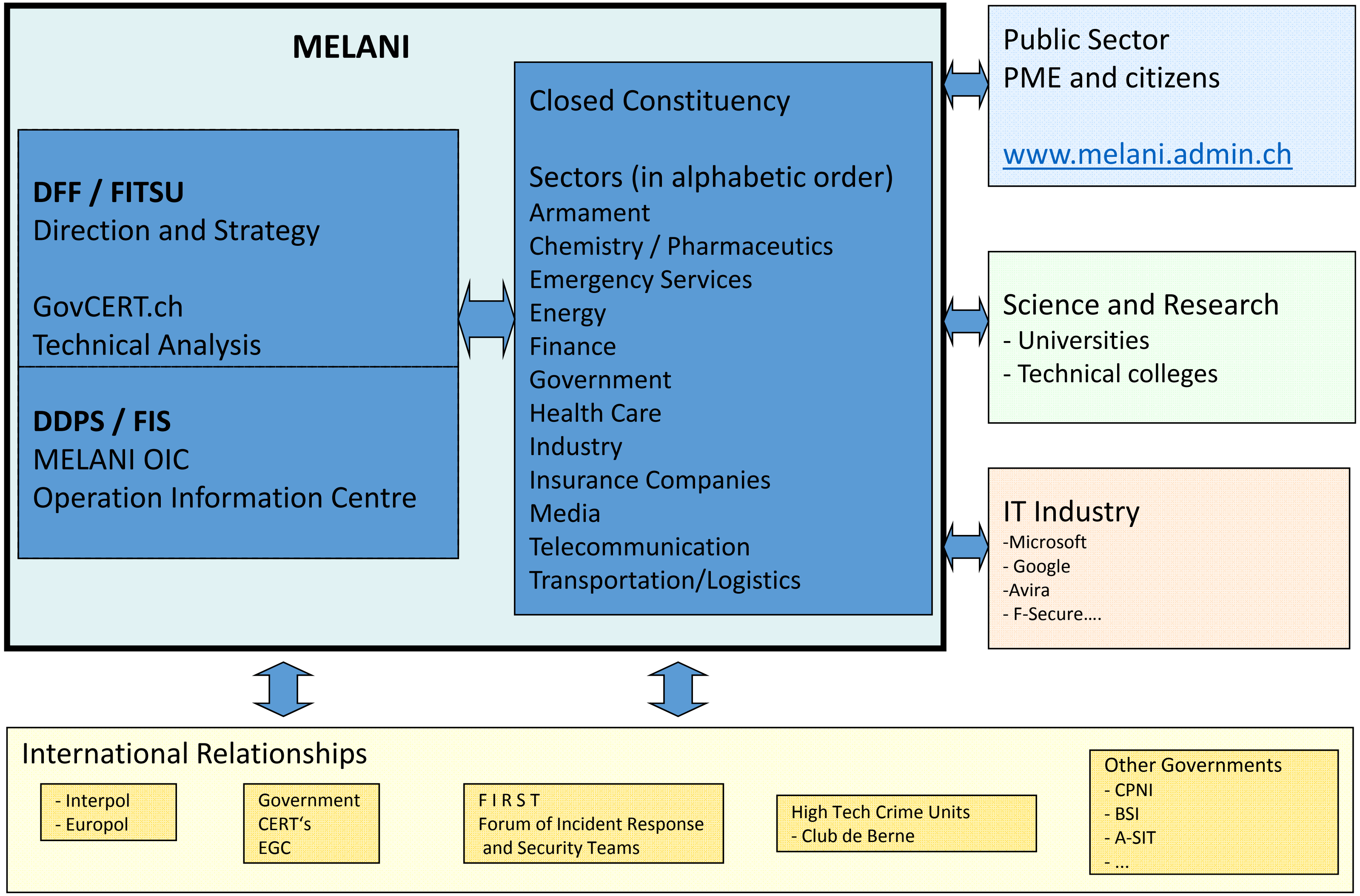
- Introducing MELANI
- Current Situation
- Does it matter to us?
- What can/should we do?
- Questions

Mandate / PPP



	SCHWEIZERISCHER BUNDESRAT CONSEIL FÉDÉRAL SUISSE CONSIGLIO FEDERALE SVIZZERO	Beschluss Décision Decisione	20. August 2003

Create and operate a Reporting and Analysis Centre for Information Assurance MELANI with the purpose to protect Swiss Critical Infrastructures from Cyber-Attacks



MELANI

DFF / FITSU
Direction and Strategy

GovCERT.ch
Technical Analysis

DDPS / FIS
MELANI OIC
Operation Information Centre

Closed Constituency

Sectors (in alphabetic order)
Armament
Chemistry / Pharmaceutics
Emergency Services
Energy
Finance
Government
Health Care
Industry
Insurance Companies
Media
Telecommunication
Transportation/Logistics

Public Sector
PME and citizens

www.melani.admin.ch

Science and Research
- Universities
- Technical colleges

IT Industry
-Microsoft
- Google
-Avira
- F-Secure….

International Relationships

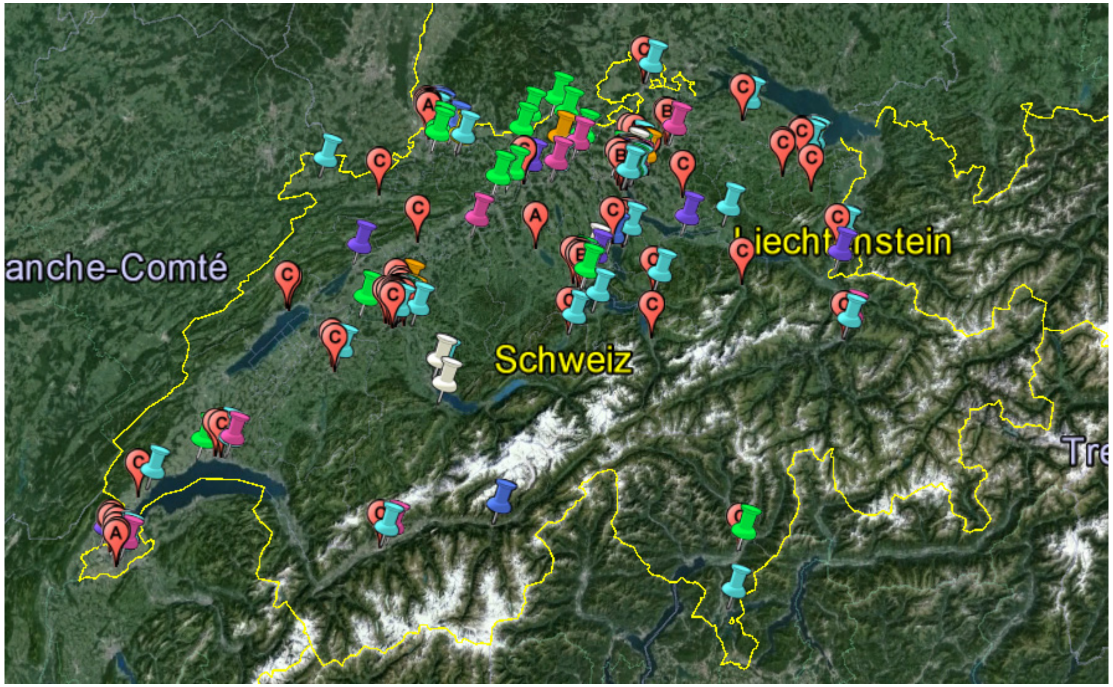
- Interpol
- Europol

Government
CERT's
EGC

FIRST
Forum of Incident Response and Security Teams

High Tech Crime Units
- Club de Berne

Other Governments
- CPNI
- BSI
- A-SIT
- …



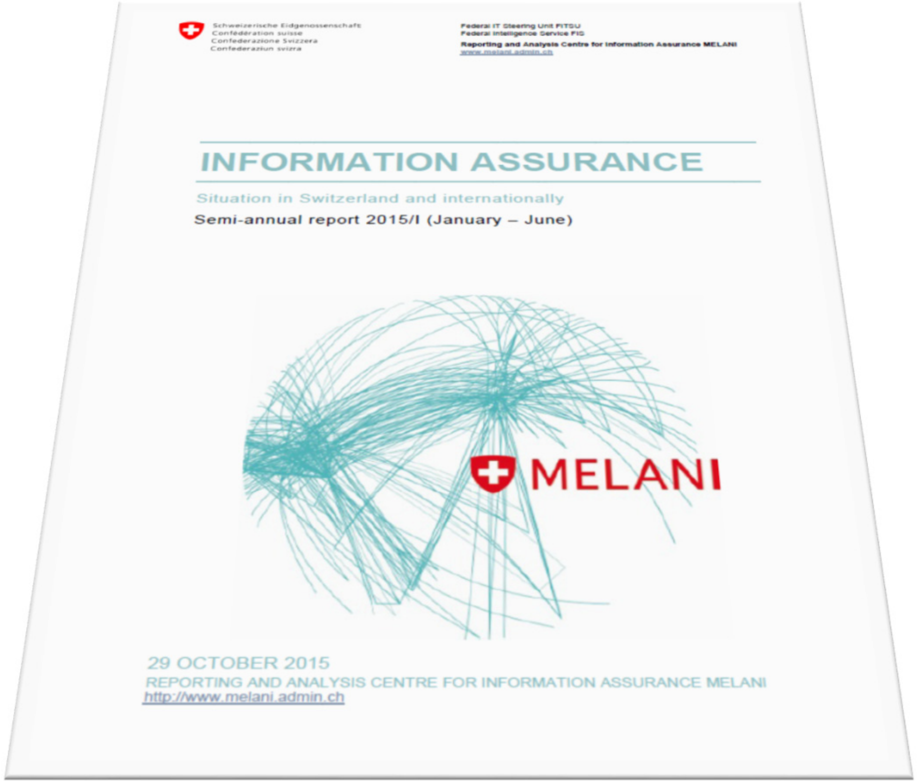
191 companies within the Closed Constituency (as of: 2016-06-03)

Emergency Services
Chemistry / Parmaceutics
Energy
Finance

Health Care
Industry
Media
Armament
Telecommunication

A Transportation/Logistics
B Insurance Companies
C Government (federal/cantonal/cities)

Public Products: Semi annual report



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal IT Steering Unit FITSU
Federal Intelligence Service FIS
Reporting and Analysis Centre for Information Assurance MELANI
www.melani.admin.ch

INFORMATION ASSURANCE

Situation in Switzerland and internationally

Semi-annual report 2015/I (January – June)

29 OCTOBER 2015

REPORTING AND ANALYSIS CENTRE FOR INFORMATION ASSURANCE MELANI

http://www.melani.admin.ch

Public Products: Newsletters and Papers

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

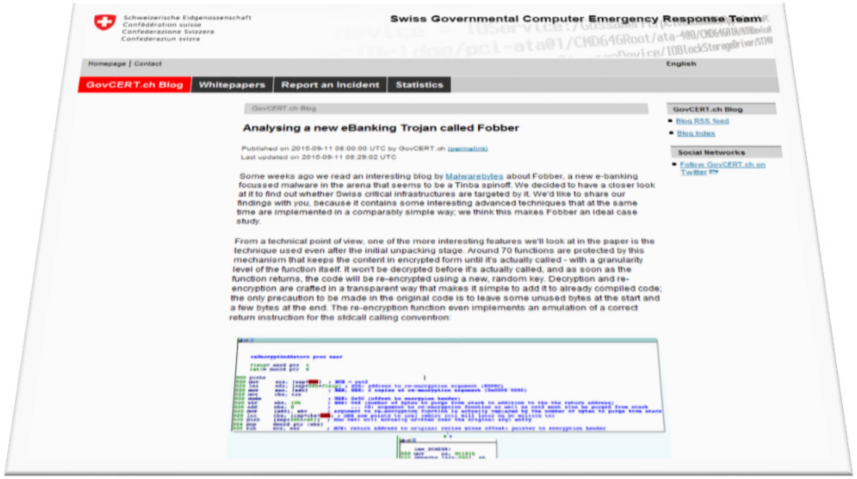
Informatiksteuerungsorgan Bund ISB
Nachrichtendienst des Bundes NDB
Melde- und Analysestelle Informationssicherung MELANI
www.melani.admin.ch

Checkliste und Anleitung

Massnahmen zum Schutz von Industriellen Kontrollsystemen (ICS)

29. Oktober 2013

Public Products: GovCERT.ch Blog



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Governmental Computer Emergency Response Team

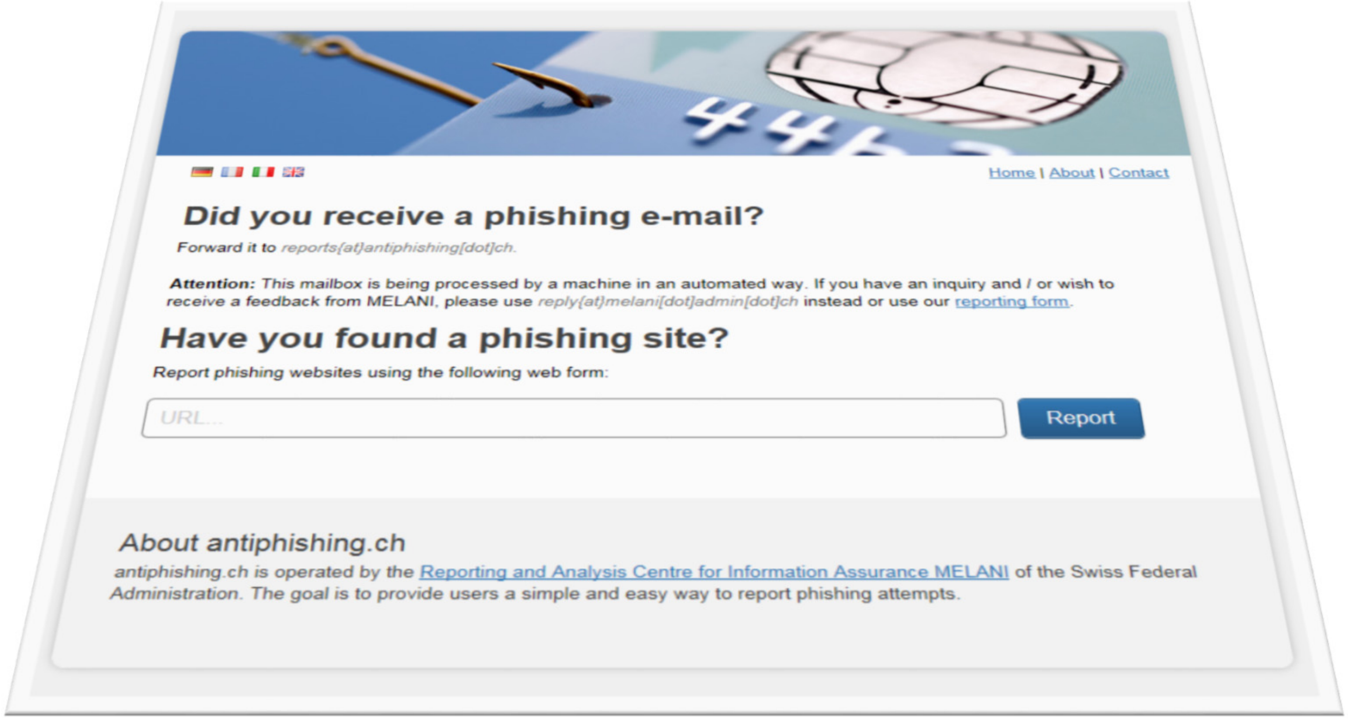
Analysing a new eBanking Trojan called Fobber

Published on 2015-09-11 08:00:00 UTC by GovCERT.ch (permalink)
Last updated on 2015-09-11 08:29:02 UTC

Some weeks ago we read an interesting blog by Malwarebytes about Fobber, a new e-banking focussed malware in the arena that seems to be a Tinba spinoff. We decided to have a closer look at it to find out whether Swiss critical infrastructures are targeted by it. We'd like to share our findings with you, because it contains some interesting advanced techniques that at the same time are implemented in a comparably simple way; we think this makes Fobber an ideal case study.

From a technical point of view, one of the more interesting features we'll look at in the paper is the technique used even after the initial unpacking stage. Around 70 functions are protected by this mechanism that keeps the content in encrypted form until it's actually called - with a granularity level of the function itself. It won't be decrypted before it's actually called, and as soon as the function returns, the code will be re-encrypted using a new, random key. Decryption and re-encryption are crafted in a transparent way that makes it simple to add it to already compiled code; the only precaution to be made in the original code is to leave some unused bytes at the start and a few bytes at the end. The re-encryption function even implements an emulation of a correct return instruction for the stdcall calling convention:

Public Products: antiphishing.ch



Did you receive a phishing e-mail?

Forward it to *reports{at}antiphishing[dot]ch*.

Attention: This mailbox is being processed by a machine in an automated way. If you have an inquiry and / or wish to receive a feedback from MELANI, please use *reply{at}melani[dot]admin[dot]ch* instead or use our reporting form.

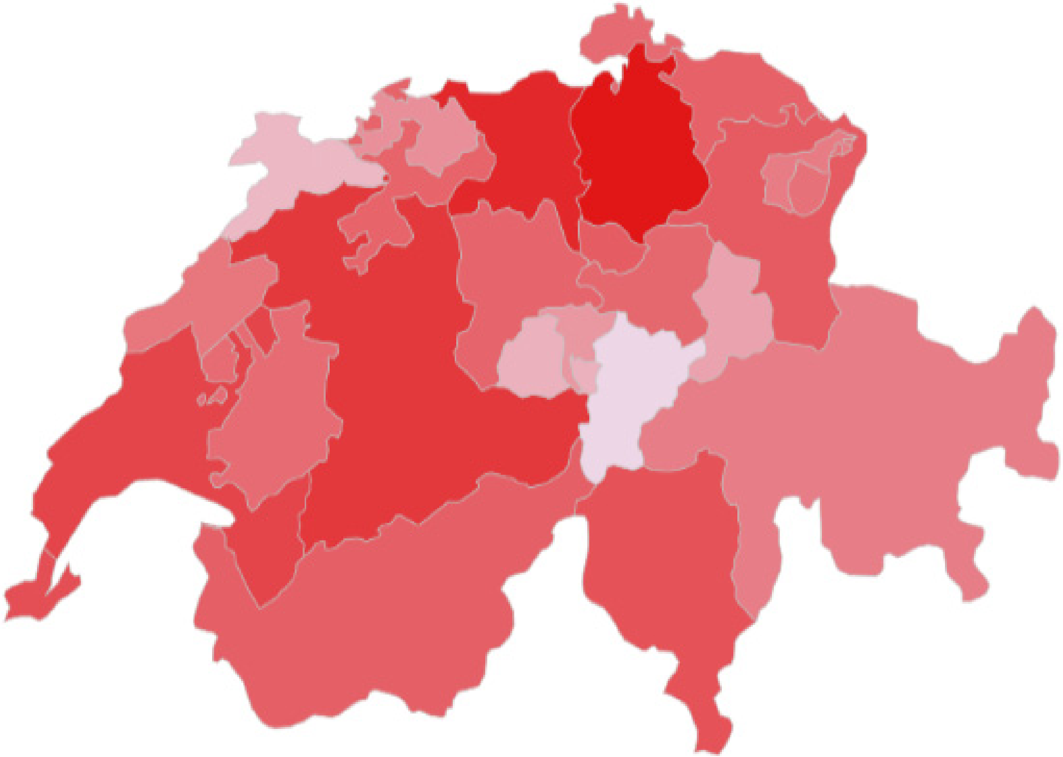
Have you found a phishing site?

Report phishing websites using the following web form:

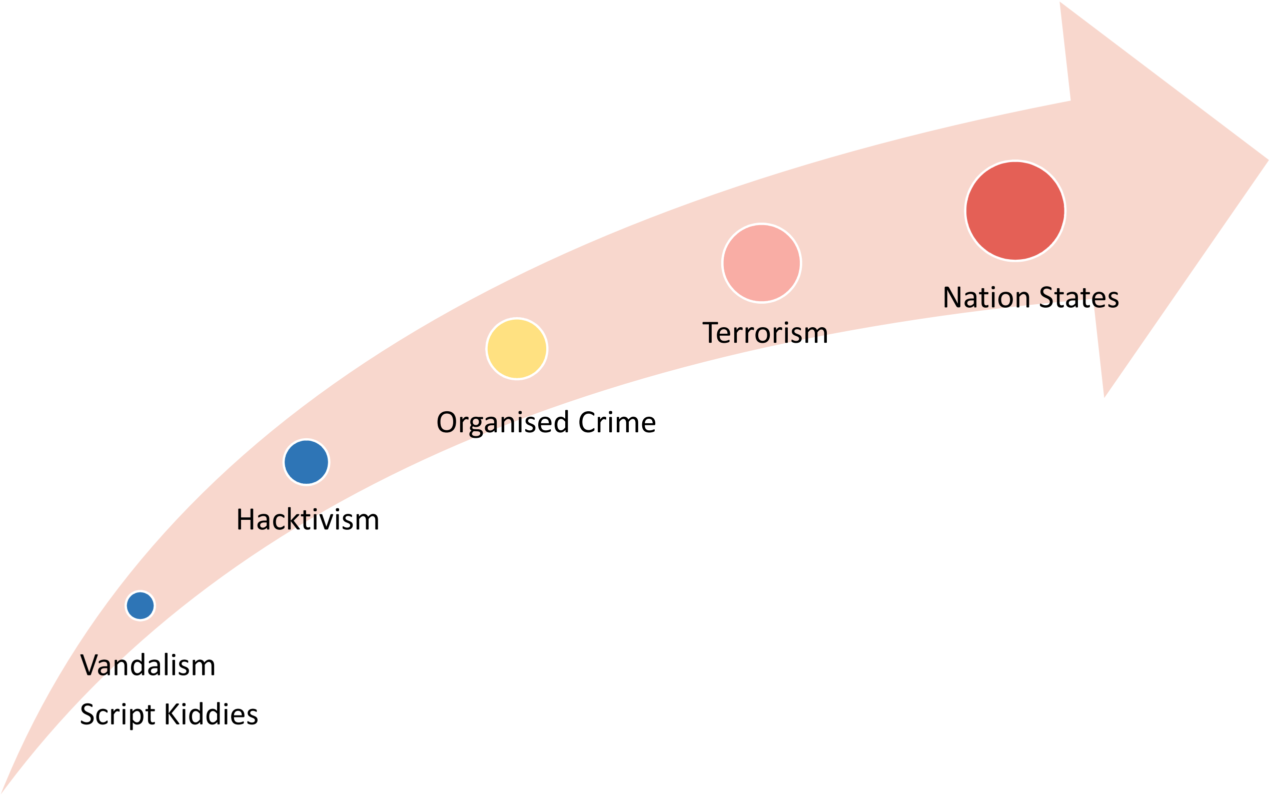
About antiphishing.ch

antiphishing.ch is operated by the Reporting and Analysis Centre for Information Assurance MELANI *of the Swiss Federal Administration. The goal is to provide users a simple and easy way to report phishing attempts.*

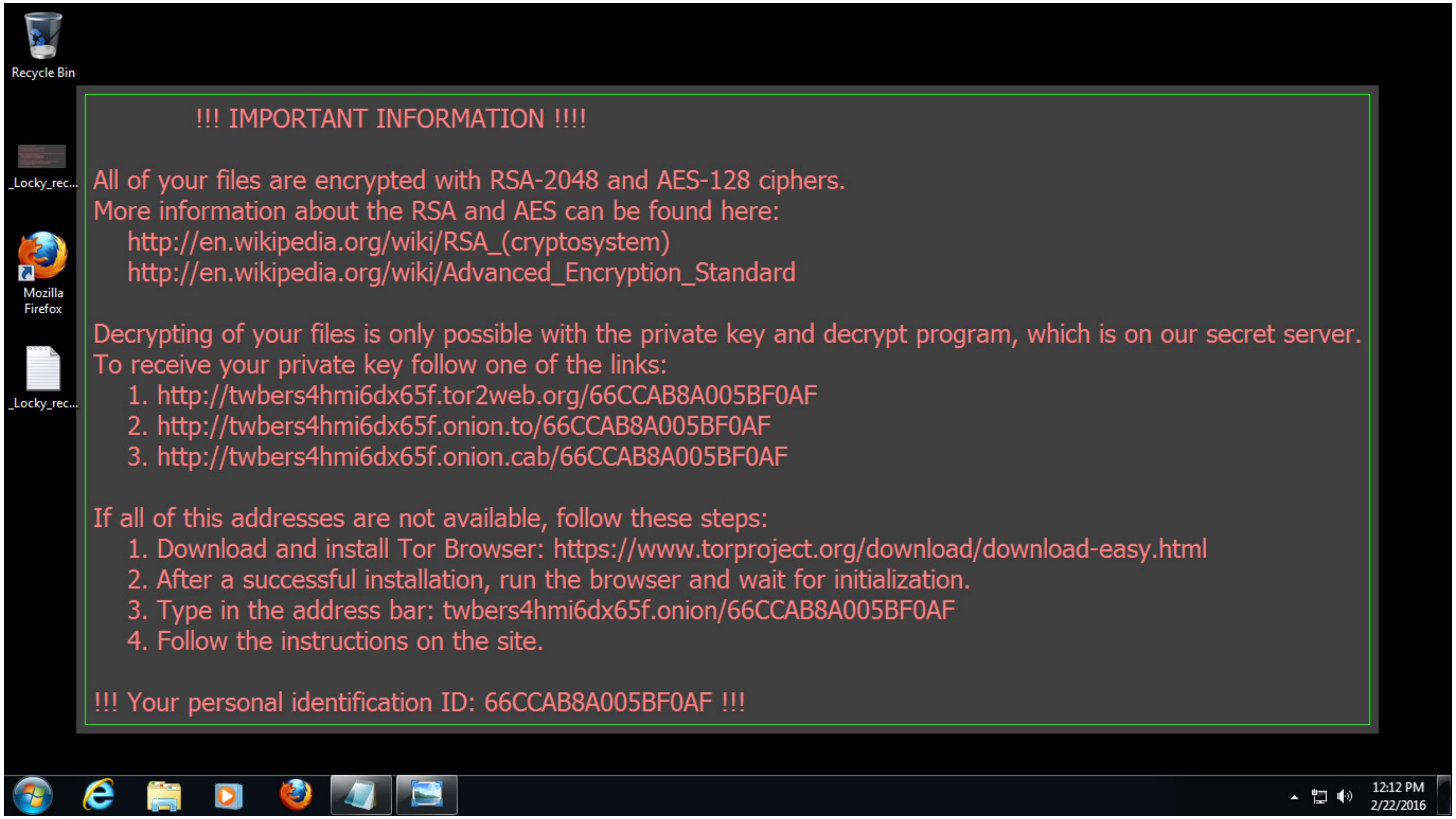
Current Situation



Cyber Actors



Ransomware



!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

1. http://twbers4hmi6dx65f.tor2web.org/66CCAB8A005BF0AF
2. http://twbers4hmi6dx65f.onion.to/66CCAB8A005BF0AF
3. http://twbers4hmi6dx65f.onion.cab/66CCAB8A005BF0AF

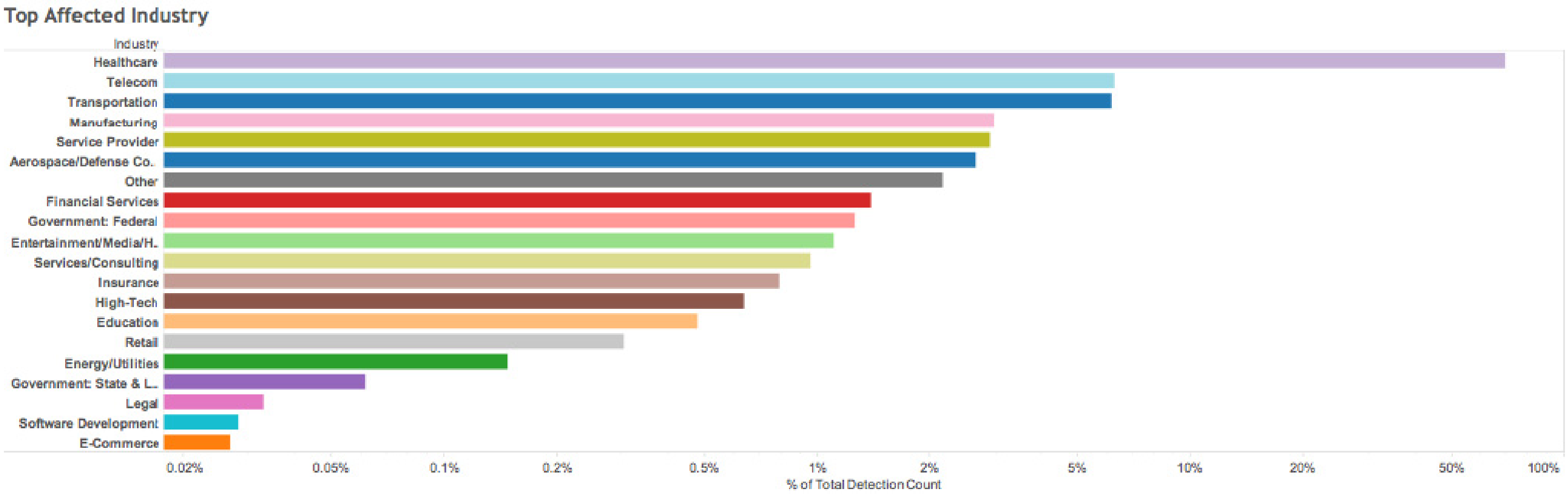
If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: twbers4hmi6dx65f.onion/66CCAB8A005BF0AF
4. Follow the instructions on the site.

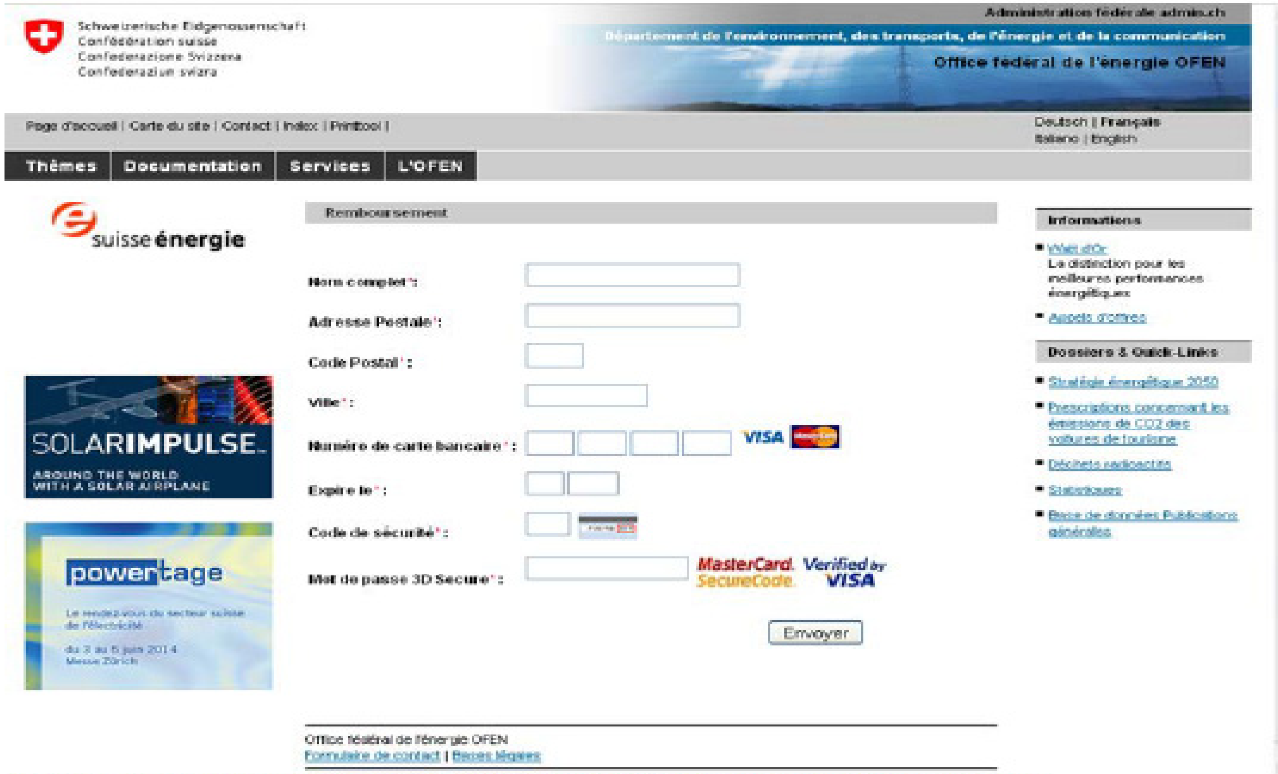
!!! Your personal identification ID: 66CCAB8A005BF0AF !!!

Ransomware

August 2016 FireEye



Social-Engineering



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Administration fédérale admin.ch

Département de l'environnement, des transports, de l'énergie et de la communication

Office fédéral de l'énergie OFEN

Remboursement

Nom complet*:

Adresse Postale*:

Code Postal*:

Ville*:

Numéro de carte bancaire*:

Expire le*:

Code de sécurité*:

Mot de passe 3D Secure*:

Informations

- Watt d'Or
  La distinction pour les meilleures performances énergétiques
- Appels d'offres

Dossiers & Quick-Links

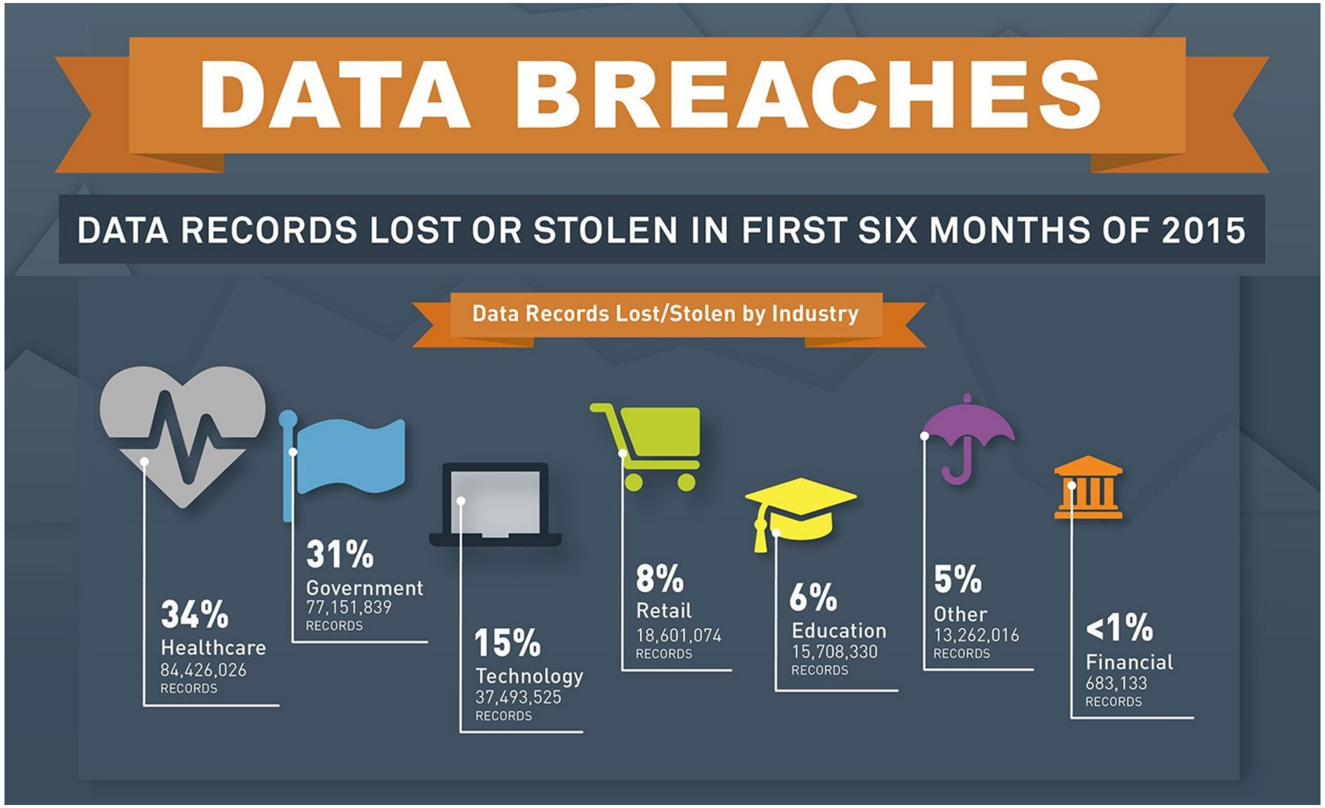
- Stratégie énergétique 2050
- Prescriptions concernant les émissions de CO2 des voitures de tourisme
- Déchets radioactifs
- Statistiques
- Base de données Publications générales

Office fédéral de l'énergie OFEN
Formulaire de contact | Bases légales

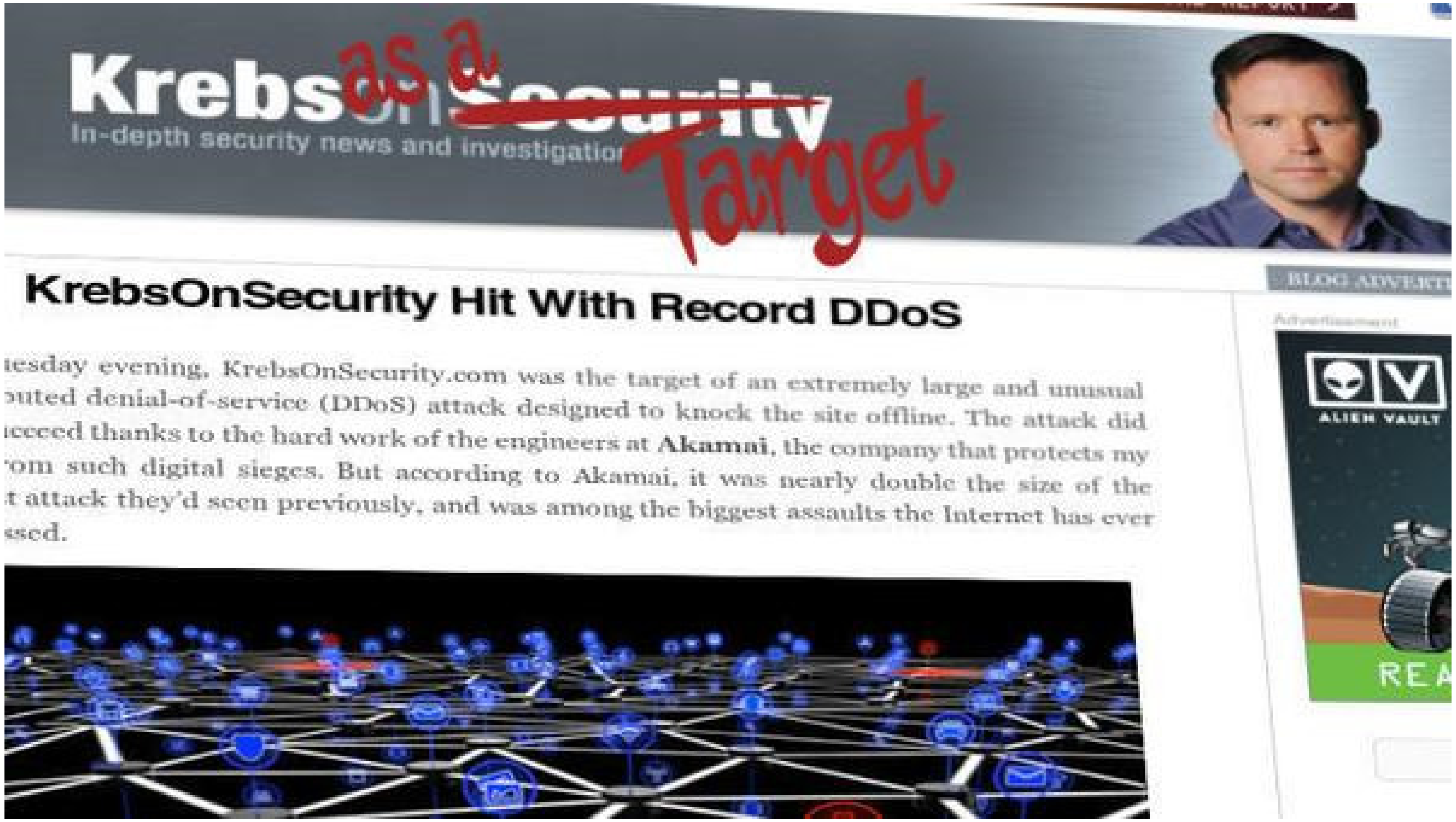
Figur 2: Phishingseite, die vorgibt vom Bundesamt für Energie zu stammen

- Phishing
- Sextortion
- CEO-Fraud
- ………

Data Breaches



DDOS



KrebsOn~~Security~~ as a Target

In-depth security news and investigation

KrebsOnSecurity Hit With Record DDoS

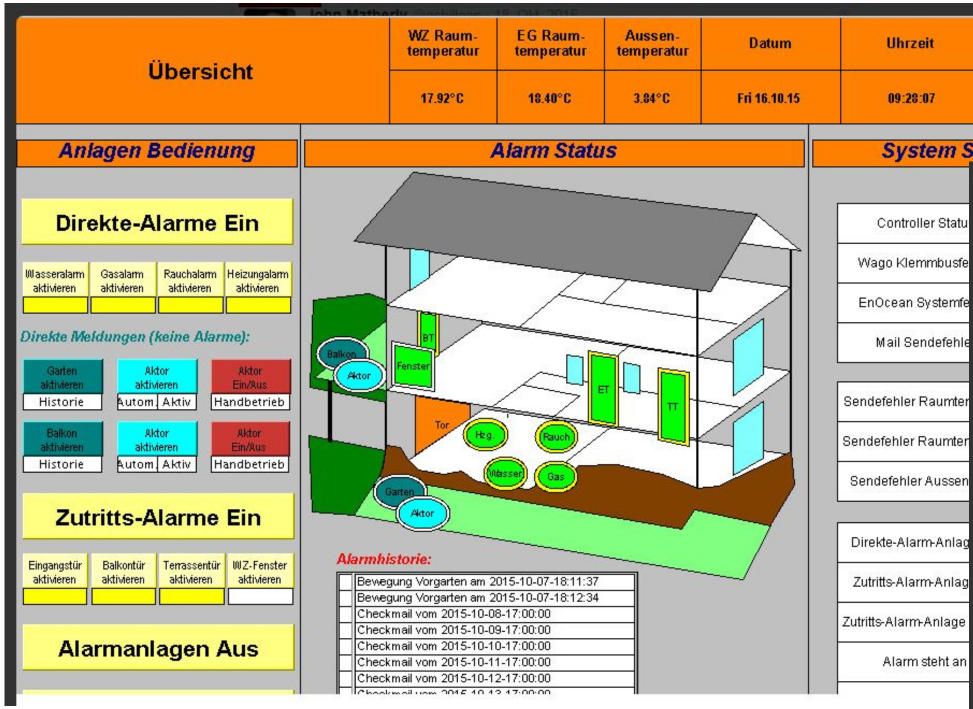
uesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual
outed denial-of-service (DDoS) attack designed to knock the site offline. The attack did
icceed thanks to the hard work of the engineers at **Akamai**, the company that protects my
rom such digital sieges. But according to Akamai, it was nearly double the size of the
t attack they'd seen previously, and was among the biggest assaults the Internet has ever
ssed.

Internet of Things (IoT)

IoT Home Routers Botnet
Leveraged in Large **DDoS Attack**

25,000 CCTV Cameras Hacked
Massive DDoS Attack Launched

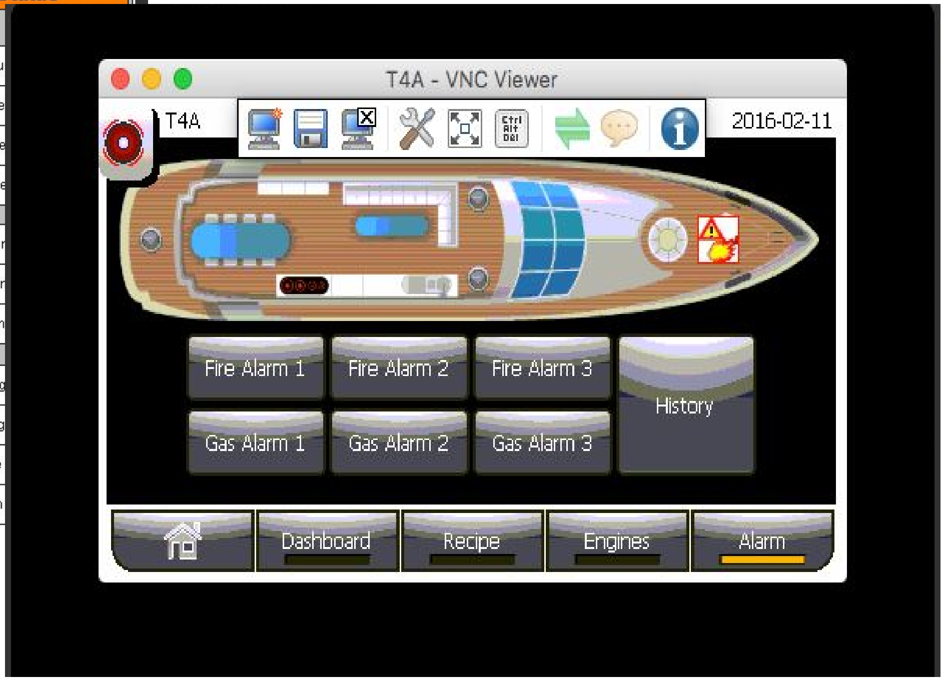
Internet of Things (IoT)



Übersicht	WZ Raum-temperatur	EG Raum-temperatur	Aussen-temperatur	Datum	Uhrzeit
	17.92°C	18.40°C	3.84°C	Fri 16.10.15	09:28:07

Alarmhistorie:

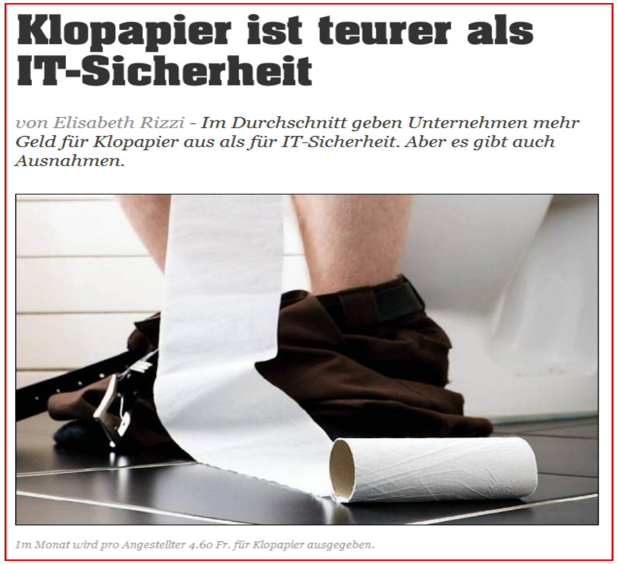
☐	Bewegung Vorgarten am 2015-10-07-18:11:37
☐	Bewegung Vorgarten am 2015-10-07-18:12:34
☐	Checkmail vom 2015-10-08-17:00:00
☐	Checkmail vom 2015-10-09-17:00:00
☐	Checkmail vom 2015-10-10-17:00:00
☐	Checkmail vom 2015-10-11-17:00:00
☐	Checkmail vom 2015-10-12-17:00:00



FITSU / FIS

Reporting and Analysis Centre for Information Assurance MELANI

Why is the adversary still winning?



Klopapier ist teurer als IT-Sicherheit

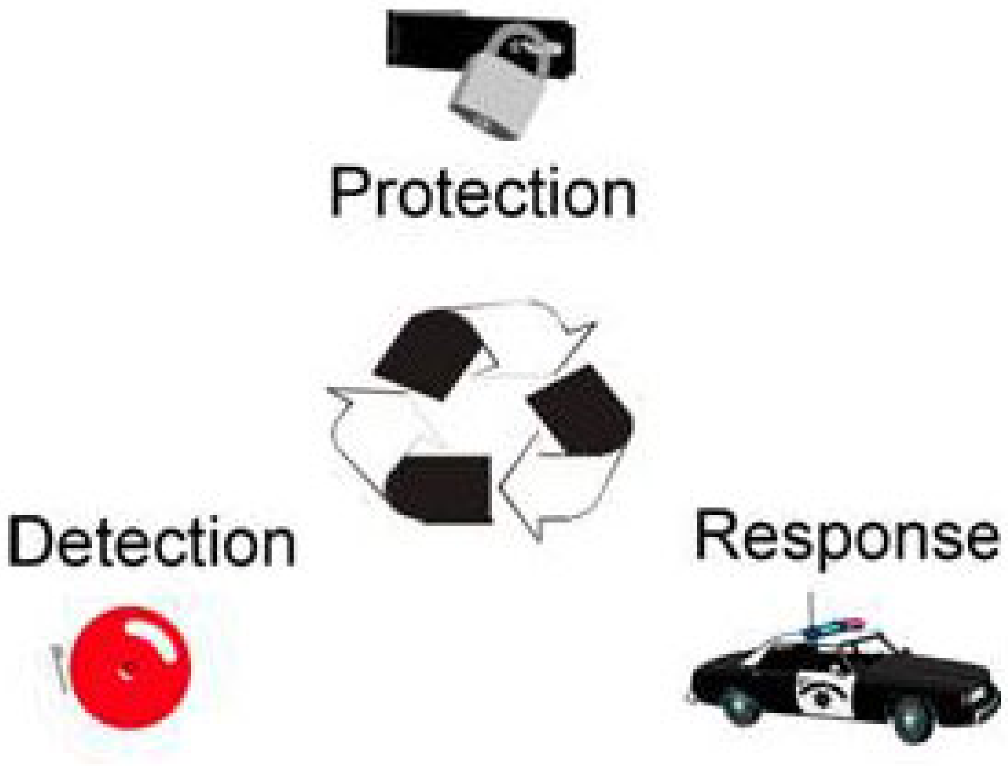
von Elisabeth Rizzi - Im Durchschnitt geben Unternehmen mehr Geld für Klopapier aus als für IT-Sicherheit. Aber es gibt auch Ausnahmen.

Im Monat wird pro Angestellter 4.60 Fr. für Klopapier ausgegeben.

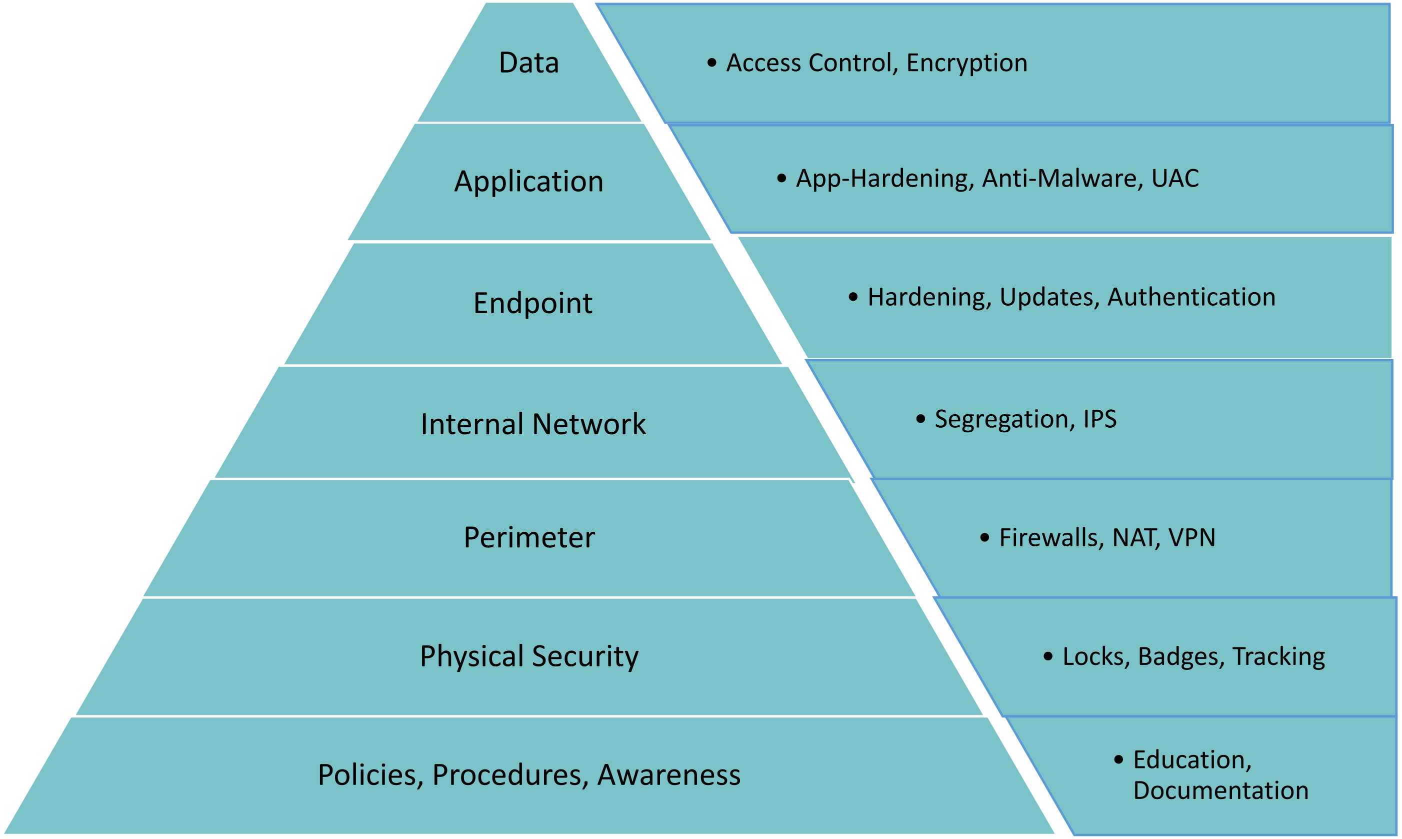
Monthly cost (average per capita):

Toilet Paper:	Fr. 4.60
E-Mail-Security:	Fr. 2.70

Protection vs. Detection vs. Response



‘Defense in Depth’



Data	• Access Control, Encryption
Application	• App-Hardening, Anti-Malware, UAC
Endpoint	• Hardening, Updates, Authentication
Internal Network	• Segregation, IPS
Perimeter	• Firewalls, NAT, VPN
Physical Security	• Locks, Badges, Tracking
Policies, Procedures, Awareness	• Education, Documentation

Change of Perception?

Thank you for your attention

Daniel Rudin
Sector Advisor
ICS MELANI / GovCERT.ch

Schwarztorstrasse 59
3003 Bern