

Protection contre les cyberrisques: où trouver de l'appui et comment envisager la défense

**Conférence protection population / Cyberrisques
EPFL – 10.11.2017**

Mathieu Simonin, Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

Le constat: un risque ne pouvant être ignoré par aucune entreprise ou administration

- Des attaques sophistiquées, ciblant des informations précises et mobilisant des ressources illimitées
- Des criminels à la recherche du meilleur retour sur investissement, voulant accéder à de l'argent en:
 - Prenant le contrôle de systèmes informatiques (maliciels)
 - Manipulant leur interlocuteur (ingénierie sociale)
 - Exerçant un chantage (cyber extorsion)
- Et tous les autres: hacktivistes, script kiddies, etc.
- Les entreprises/administrations sont en première ligne
- Où trouver de l'appui ? Comment envisager la défense ?



Au cœur de ces problématiques: MELANI

- Active depuis 2004
- Répartie entre DDPS et DFF; comprenant GovCERT
- Protection des infrastructures critiques comme mission première
- Prestations pour la population et les entreprises
- PPP
- Participation volontaire des partenaires, MELANI n'est pas un régulateur
- Subsidiarité



Tâches de MELANI

- **Observation de la situation nationale/recueil d'information dans un but de :**
 - Prévention (moyen/long terme)
 - Alerte/Incident handling (court-terme)
- **Cercle fermé** de MELANI :
 - Établissement et maintien d'un **réseau** avec les opérateurs des infrastructures critiques
 - Soutien des opérateurs des infrastructures critiques : partage d'information; évaluation de la menace; soutien en cas d'incident
- **Cercle ouvert** de MELANI :
 - Mesures de prévention pour les PME et la population
 - **Prestations** visant à diminuer l'impact de différentes menaces



Un point de contact pour le public

Le Conseil fédéral > MELANI >

Page d'accueil Plan du site Contact DE FR IT EN

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Centrale d'enregistrement et d'analyse
pour la sûreté de l'information MELANI

Thèmes actuels
Comment se protéger?
Documentation
Formulaire d'annonce
Généralités concernant MELANI

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI > Formulaire d'annonce > Je souhaiterais effectuer une autre annonce

← La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

Formulaire d'annonce

Cas fréquemment annoncés et formulaire

Utilisation

Je souhaiterais effectuer une autre annonce

Email

Organisation

Votre message *

Je n'attends pas de réponse!

Envoyer

SRC / UPIC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

5



Pourquoi annoncer des cas?

- Des conseils de prévention généraux
- Une expertise technique
- Profiter d'une vue d'ensemble de la situation
- Aussi un service d'orientation
- Pour nous, un senseur incontournable en vue de mesures de prévention
- Permet de diminuer l'impact des menaces

SRC / UPIC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

6



Action contre les sites de phishing

https://www.antiphishing.ch/fr/

antiphishing.ch

Page d'accueil | Informations | Contact

Vous avez reçu un e-mail de phishing?

Transmettez les e-mails de phishing à reports@antiphishing.ch.

Attention: Les e-mails envoyés à cette adresse ne sont pas lus mais traités automatiquement. Si vous avez une question et/ou attendez un retour de MELANI, merci d'écrire à reply@melani.punkt.admin.punkt.ch ou d'utiliser le [formulaire d'annonce MELANI](#).

Vous avez découvert un site de phishing?

Annoncez les adresses des sites de phishing à travers notre formulaire en ligne:

URL...

SRC / UPIC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

7



Lutte contre les maliciels

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Governmental Computer Emergency Response Team

Homepage | Contact

GovCERT.ch Blog | Whitepapers | Report an Incident | Statistics

English

Statistics > Malware Families

Infections per Malware Family

gozi downadup kellihos ZeroAccess timba
 downloadadbot-mxb dyrc intel darknet sality zeus torpig
 others

© GovCERT.ch

Show graph in full screen

About the data: These statistics originate from the DroneDB, a database containing infected systems in Switzerland that have been active the last 48h. This database is fed by different sources, mostly DNS sinkholes operated by different organizations, where infected clients connect to instead of the real C&C servers. This data is aggregated and filtered for all Swiss IP space known to MELANI / GovCERT. The different malware families are sometimes hard to distinguish as there does not exist any international naming schema. It is important to note that these numbers just show the tip of the iceberg, as our database only contains data from sinkholed Command and Control servers.

Action recommended: MELANI/GovCERT provides the list of infected system per AS (Autonomous System) to different ISPs. Any operator of a network owning its own AS may get this list in order to inform the affected customers within his own network boundary. The goal must be to reduce the number of infected systems, as well as the duration of an infection. GovCERT provides timely information about infections and the ISPs need to inform their customers. For doing so they need to have adequate abuse- and helpdesk resources. This information must be done by the respective ISPs as GovCERT has no information about who uses which IP at a given time.

Source: <http://www.govcert.ch>

SRC / UPIC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

8



Information et prévention générale

Documentat
Lettre d'info

https://ww

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun Svizra

Département fédéral des finances DFF
Unité de pilotage informatique de la Confédération UPIIC
Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI
GovCERT.ch

Mesures à prendre contre les attaques DDoS

MELANI / GovCERT.ch

Version:	v1.00
Auteur:	MELANI / GovCERT.ch

Disclaimer: tous les logos utilisés dans le présent document sont des marques déposées ou propriété du détenteur correspondant. Conformément aux licences dites Creative Commons (CC BY-ND 3.0), les présentes instructions peuvent être réutilisées par des tiers.

<http://creativecommons.org/licenses/by-nd/3.0/>

MELANI / GovCERT.ch page 1 sur 4 20 mai 2015

Les escrocs prennent
des mesures d'activation

E-ba
moy

ons relatives à la
ion des malicieux
comportement

d'information que les escrocs visent
mobiles utilisés pour l'e-banking.
es à leur envoyer une copie de la
mettant d'activer l'authentification

erner les moyens
ngénierie sociale et en utilisant
ces attaques les utilisateurs de
ndamment du système
bile (Android, iOS).

enregistrement et d'analyse pour
se des attaques qui cherchent à
onnées d'activation du processus
nent souvent la forme d'une
onnecte à l'aide d'un appareil
ser ou photographier avec une
n ou SecureSign. L'appareil utilisé
risé pour la procédure de
transmet en général ces données
voie postale. Les escrocs essaient
en manipulant leurs victimes et
e ou une photographie qui doit

SRC / UPIC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

9



Appréhension du risque

- La première étape est une prise de conscience: cela n'arrive pas qu'aux autres!
- A partir de là, il est nécessaire d'identifier les (ses) risques
- Comme préalable à cette réflexion, se connaître soi-même: quelles données, quelle valeur, quelle possibilité d'accès...
- Chaque entreprise n'aura pas non plus les mêmes priorités
- De la volonté de gérer ces risques découleront des mesures technologiques, humaines, organisationnelles
- Cette prise de conscience doit se faire au niveau du management, car elle nécessitera des budgets

SRC / UPIC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

10

Répondre à une menace à multiples facettes

- De nombreux acteurs aux motivations diverses
- Consolidation de certains modes opératoires ayant fait leur preuve mais également recherche constante de nouvelles opportunités
- Face à des cybercriminels «rationnels»: se protéger c'est souvent dissuader l'attaquant
- Mais pour des attaques plus perfectionnées: la capacité à détecter l'anomalie et y répondre doit être une priorité
- Une certitude: la voie unilatérale est une impasse → face à des attaquants échangeant efficacement de l'information, le partage entre pairs et avec les autorités est primordial (modes opératoires, indicateurs, bonnes pratiques, etc.)



Merci pour votre attention

Plus d'informations sur notre site web:

<http://www.melani.admin.ch>