Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC

Etat de la Menace et Conseils Relatifs aux Rançongiciels

18.11.2021

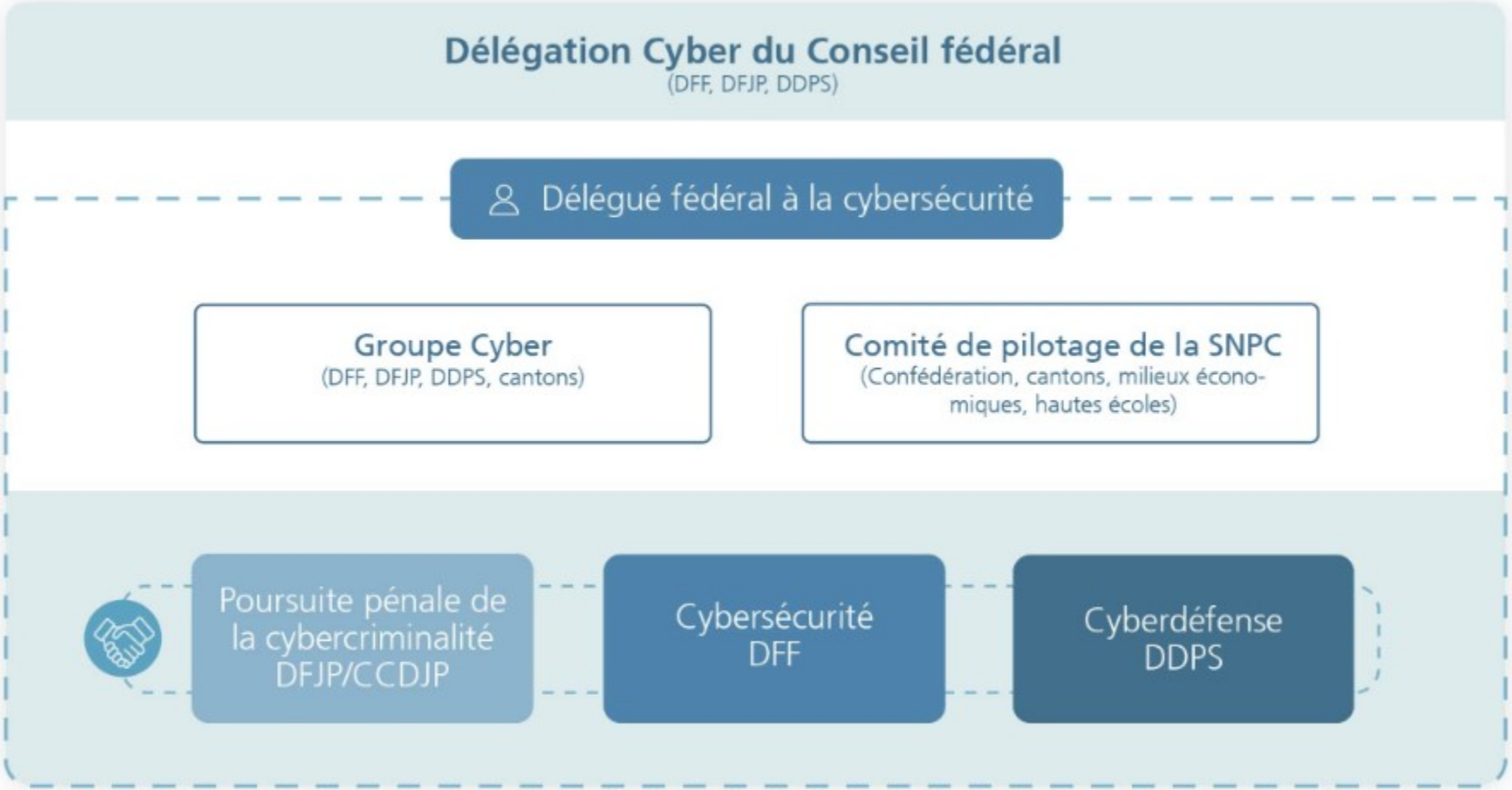
Agenda

Intervenant:
- **Alexandre Herzog**
  NCSC.ch

1	**Centre national pour la cybersécurité NCSC**
2	**Etat de la menace**
3	**Recommandations & Réponse à incident**

1. Centre national pour la cybersécurité NCSC

NCSC - Organisation de la Confédération dans le domaine des cyberrisques

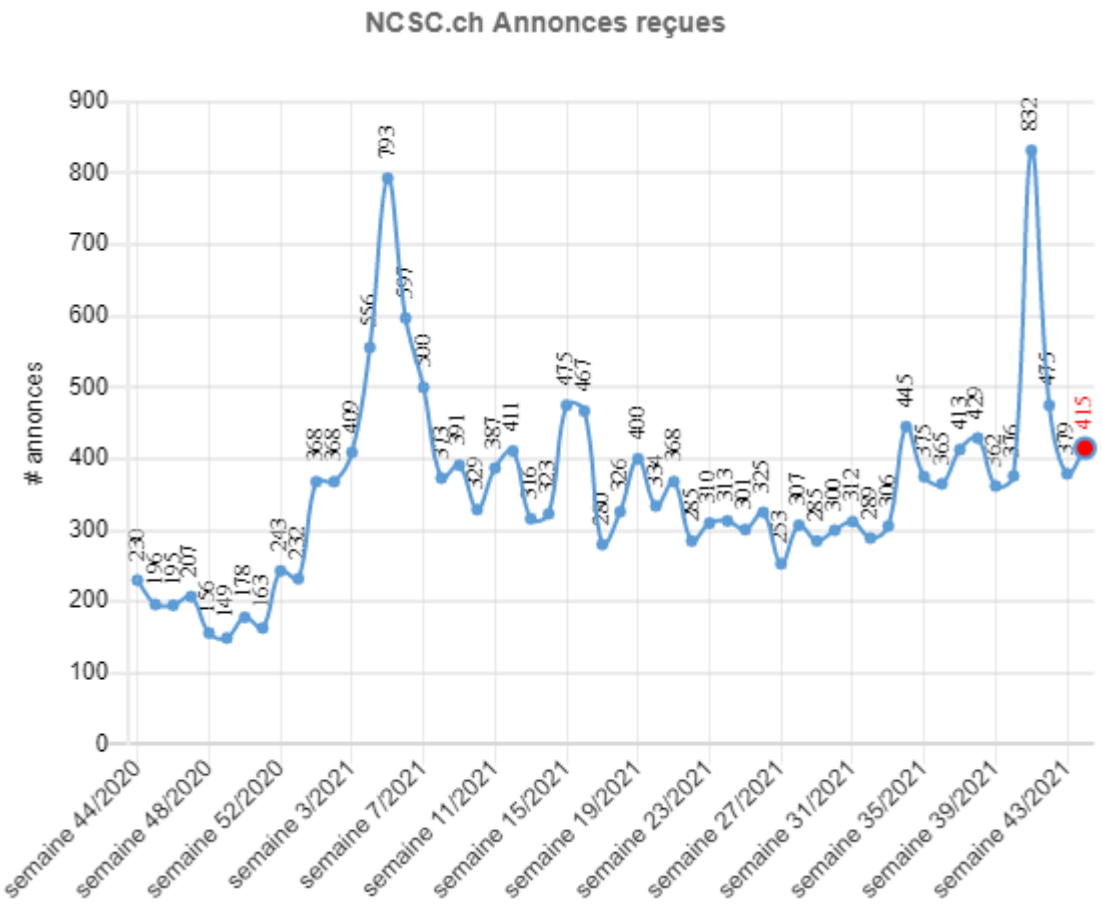


Centre national pour la cybersécurité NCSC

- Centre de compétences de la Confédération en matière de cybersécurité
- Interlocuteur pour toute question relative à la cybersécurité pour
  - Milieux économiques
  - L'administration
  - Les établissements d'enseignement
  - La population
- Responsable de la mise en œuvre coordonnée de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) pour 2018 à 2022
- Intègre des composants de MELANI, notamment l'équipe d'intervention en cas d'urgence informatique (GovCERT)

2. Etat de la menace

Etat de la menace - Signalements reçus par le NCSC

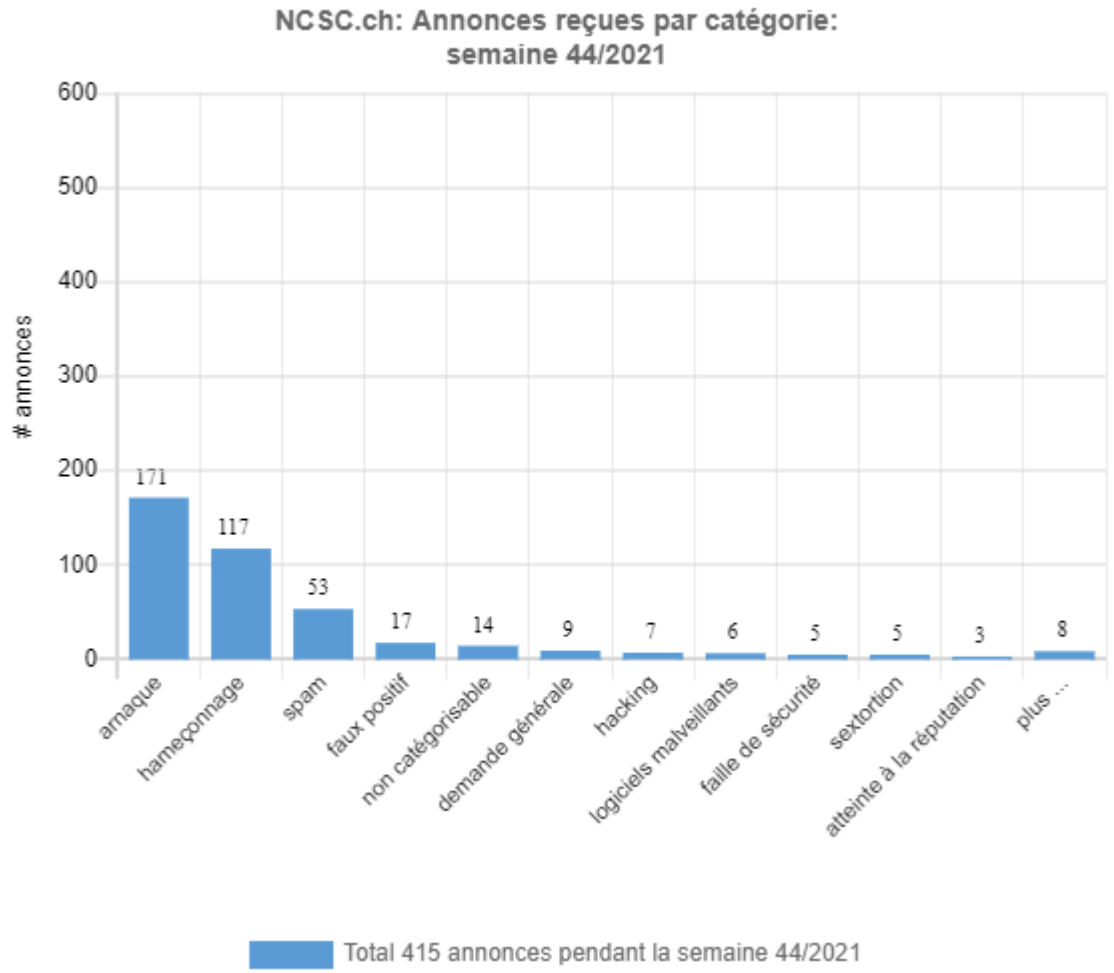


En 2020

10’834 annonces d’entreprises et de la population
dont
5924 Arnaques
416 Logiciels malveillants
165 Hacking
24 Pertes de données

Plus de 8500 réponses

Etat de la menace - Signalements reçus par le NCSC



En 2021

Plus de 16’500 annonces d’entreprises et de la population

Etat de la menace – Vue générale

- Fraudes / Arnaques
  - Faux investissements en cryptomonnaies & fraude au président
  - Autres Arnaques (phishing, sextorsion, fausses annonces etc.)
- Attaques
  - Déni de Services Distribués (DDoS)
  - «Hacking» de comptes ou de services
- Virus
  - Cheval de Troie bancaire
  - Autres virus

- **Rançongiciels**

Etat de la menace – Focus rançongiciels

- Pas nouveau, mais nouvelle ampleur depuis 2019
- Avant 2019: «petites» mais nombreuses attaques
  - Chiffrement immédiat des victimes, en règle générale faible rançon
- 2019: ciblage des entreprises
  - Mouvement latéral préalable pour augmenter l'impact (et la rançon)
  - Recherche des backups en vue de leur destruction préalable avant chiffrement
- 2020: double extorsion
  - Exfiltration des données préalable pour faire chanter les victimes
- 2021: triple extorsion & visibilité accrue
  - Augmentation des rançons et de la visibilité des attaques
  - Intérêt médiatiques accru, notamment envers les victimes n'ayant pas cédé au chantage

Etat de la menace – Focus rançongiciels

Historique des publications de MELANI / NCSC / GovCERT.ch:

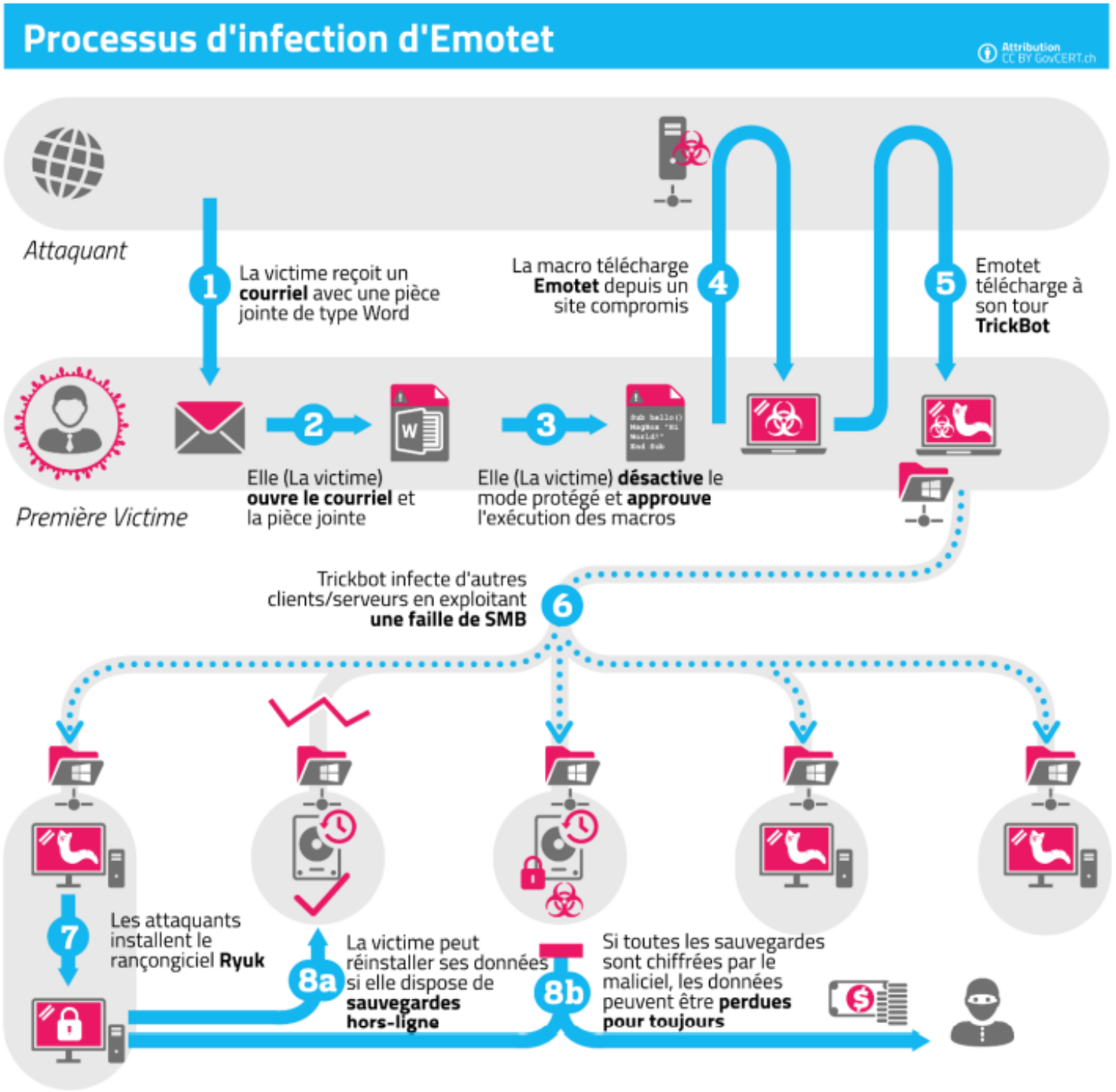
- 02.11.2017 - Les rançongiciels et les courriels abusifs envoyés au nom d'autorités sont de plus en plus nombreux
- 09.05.2019 - Severe Ransomware Attacks Against Swiss SMEs
- 09.05.2019 - Les rançongiciels menacent de plus en plus les réseaux des entreprises
- 30.07.2019 - Mise à jour rançongiciels: nouvelle façon de procéder
- 19.02.2020 - Prudence: un nombre croissant de PME victimes de rançongiciels
- 18.08.2021 - Attaques au rançongiciel réussies contre des entreprises suisses

Etat de la menace

Source
https://govcert.ch/

Rapport semestriel
MELANI 2020/2

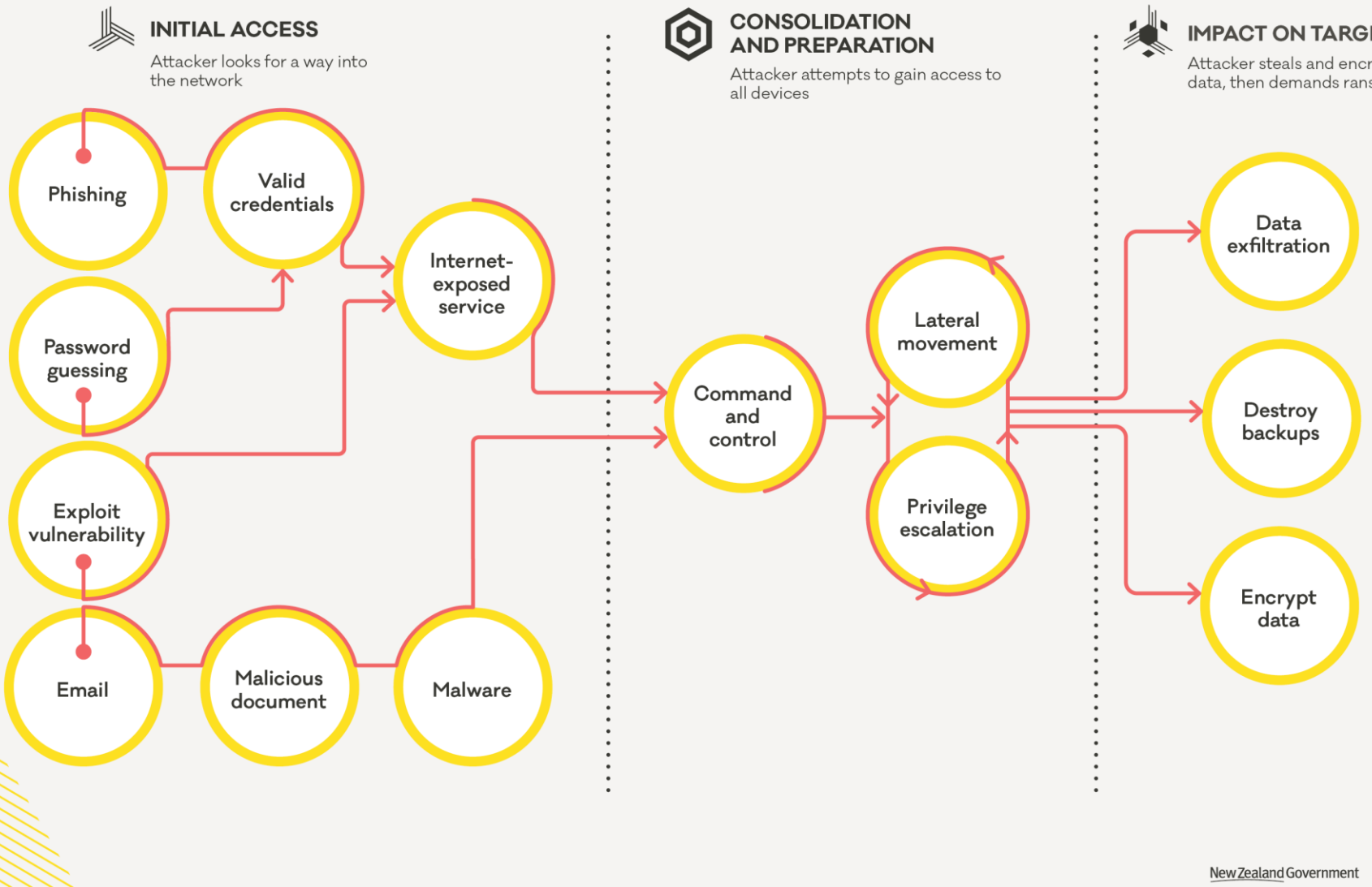
Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC



LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.



New Zealand Government

Source
https://www.cert.govt.nz/

Etat de la menace – Rançongiciels été 21

- Moins de cas liés à une intrusion initiale par malware
- Beaucoup de cas lié à des services exposés sur Internet sans 2FA
  - L'accès distant (VPN, Citrix, RDP, …) **doit** être sécurisé avec un composant additionnel, pas uniquement nom d'utilisateur et mot de passe
- Attaque via la chaîne d'approvisionnement («Supply chain attack»)
- Votre prestataire IT devient la porte d'entrée des attaquants

Etat de la menace – Rançongiciels automne 21

- Recrudescence des maliciels délivrés par email (QuakBot, Dridex)
  - QuakBot vole des conversations de courriel légitimes dans les boîtes aux lettres des ordinateurs précédemment infectés
  - Ces conversations sont réutilisées pour appâter d'autres victimes ("email threat hijacking " ou "dynamite phishing").
  - **Retour depuis le 15.11.2021 du malware Emotet**
- La charge malicieuse est livrée soit
  - Par une pièce jointe malicieuse (fichier avec macro parfois dans un zip)
  - Par un ou plusieurs liens dans l'email, d'où un document malicieux est téléchargé

Etat de la menace – Quiz!

De: <support@clearskincentre.com>
Objet: Rép : Re: Distribution - Set [redacted]
Date: 11 novembre 2021 à 17:14:30 UTC+1
À: [redacted]

Bonjour,
Veuillez consulter le fichier ci-joint. Elle doit être intéressante

Merci.

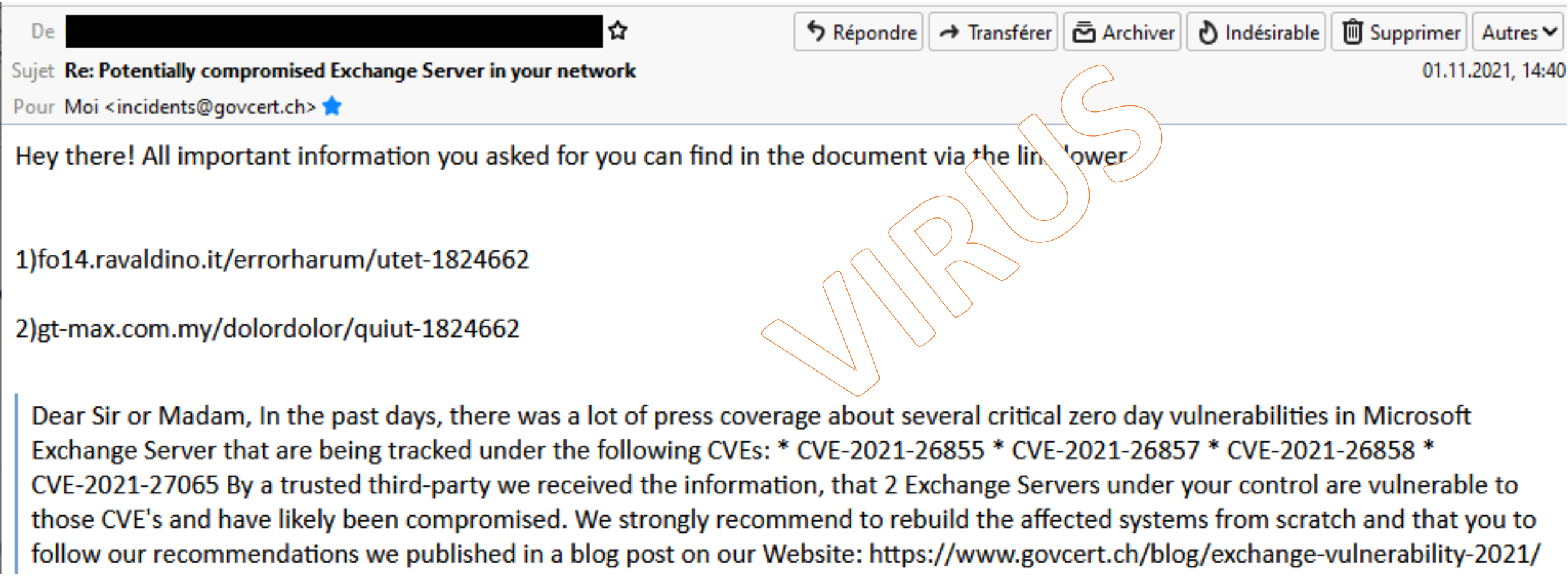
> Bonjour!
>
> Merci pour les informations, et pour la distribution. Quelle année laborieuse…
> Bon courage, et tous mes voeux,

2 pièces jointes 95.8 Ko

LOGO_[redacted] 1809264946-11112021.zip 85.5 Ko

VIRUS

Etat de la menace – Quiz!



VIRUS

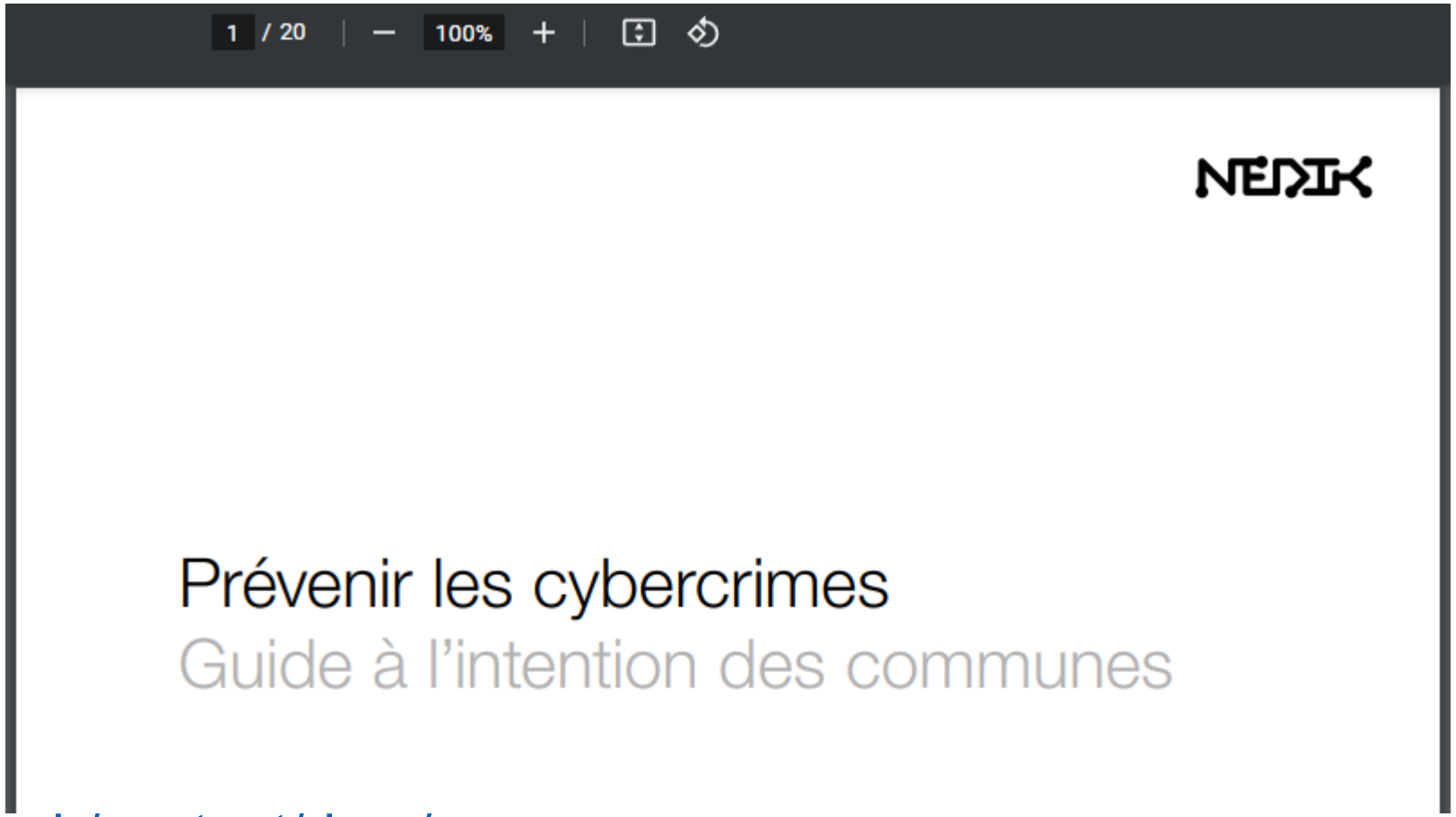
3. Recommandations & Réponse à incident

Bonnes pratiques contre les rançongiciels

Recommandations techniques contre les rançongiciel:
https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/ransomware-8.html

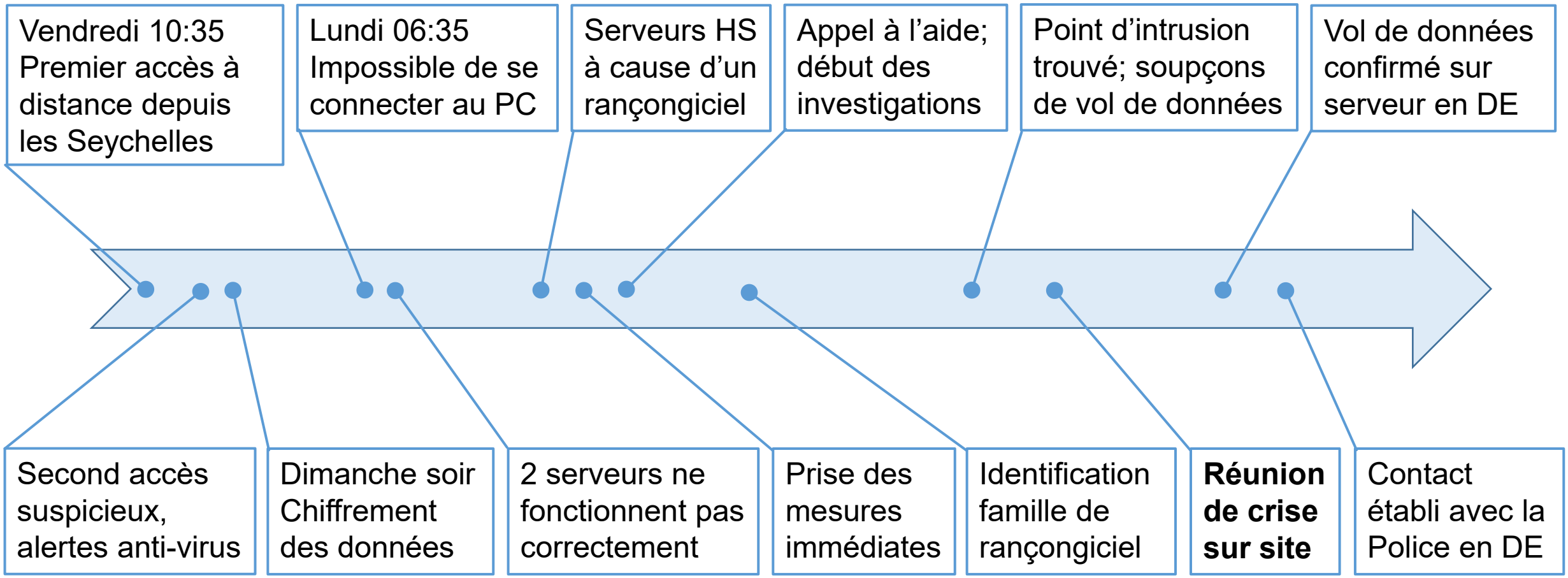
- Gestion des correctifs et des cycles de vie
- Sécurisation des accès à distance
- Blocage des pièces jointes à risque dans les courriels
- Sauvegardes hors ligne

Bonnes pratiques globale



Source:
https://www.svs.admin.ch/content/dam/svs-internet/fr/documents/Guide%20a%20l%20intention%20des%20communes.pdf

Réponse à incident – Exemple fictif



Réponse à incident – Elements clés

- Cet exemple ne couvre que les premières heures de la réponse à incident
- Différenciation Réponse à Incident & Gestion de Crise
  - Le sprint de la réponse à incident est déjà bien lancé
  - Le marathon de la gestion de crise ne fait que de débuter

- Etapes avant / débutant une réponse à incident
  - Identifier et comprendre des anomalies
  - Notification par un tiers
  - Ou alors directement données / outils de travail chiffrées
- **Une détection précoces des anomalies permet d'éviter des crises!**

Réponse à incident – Pourquoi impliquer les autorités (Police, NCSC. …)?

- Obtenir de l'aide rapidement
- Gagner du temps au début de l'incident
- S'assurer de la préservation des preuves pour la poursuite pénale

- Montrer le bon exemple

Réponse à incident

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Classification :	MELANI BLEU / TLP AMBER
Sujet :	**Réponse aux incidents de type Ransomware**
Statut :	19 avril 2021
Auteur :	NCSC / GovCERT.ch

Ce document est destiné à un usage interne et ne doit pas être rendu public. Toutefois, il peut être mis à la disposition des entreprises concernées en Suisse aux fins de la gestion d'un cyber incident impliquant un rançongiciel.

Introduction

Le document fournit une ligne directrice pour un processus de réponse à incident efficace et efficient pour les entreprises touchées par une attaque de rançongiciel.

Mesures immédiates

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC

Résultats

Source:

https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure

12 TARGETED FOR INVOLVEMENT IN RANSOMWARE ATTACKS AGAINST CRITICAL INFRASTRUCTURE

29 October 2021

Press Release

These cyber actors represented a dangerous combination of aggressive disruption and high-stake targets

A total of 12 individuals wreaking havoc across the world with ransomware attacks against critical infrastructure have been targeted as the result of a law enforcement and judicial operation involving eight countries.

These attacks are believed to have affected over 1 800 victims in 71 countries. These cyber actors are known for specifically targeting large corporations, effectively bringing their business to a standstill.

The actions took place in the early hours of 26 October in Ukraine and Switzerland. Most of these suspects are considered high-value targets because they are being investigated in multiple high-profile cases in different jurisdictions.

As the result of the action day, over USD 52 000 in cash was seized, alongside 5 luxury vehicles. A number of electronic devices are currently being forensically examined to secure evidence and identify new investigative leads.

THE TICKING TIME BOMB OF UNDETECTED MALWARE

Quels sont les premiers gestes en cas d'incident?

Dans le canton de Vaud:

117

Contact NCSC

https://www.report.ncsc.admin.ch/fr/

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC

Conseils en cas de cyberattaque

Comme toute structure présente sur Internet, les communes peuvent être la cible des cybercriminels.

Les conséquences d'une attaque informatique peuvent être atténuées, à condition de prendre les bonnes mesures et d'agir vite... car, en matière de cybercriminalité, le temps joue contre nous.

Cette notice, à l'attention des communes et de leurs responsables informatiques, explique les premières actions à entreprendre en cas d'attaque par rançongiciel.

PS-SEC/202110.01

COMMENT RÉAGIR EN CAS D'ATTAQUE PAR RANÇONGICIEL

En cas de suspicion d'attaque par rançongiciel, des mesures urgentes doivent être prises :

1. **Isoler votre informatique de l'extérieur :** couper les connexions Internet, l'accès VPN ou tout autre accès distant.
2. **S'assurer que vos sauvegardes sont intègres** et les déconnecter du reste de votre infrastructure. Cela permettra de procéder à la restauration ultérieure des systèmes.
3. **Contacter la Police cantonale (117)** et demander l'entité cybercrime pour annoncer l'incident. Cette entité sera votre point de contact avec les autorités cantonales et vous aidera dans vos démarches (dépôt de plainte et première analyse), et impliquera les experts du Centre opérationnel de sécurité vaudois (SOC) en cas de nécessité .
4. **Une cellule de crise** doit être mise en place le plus rapidement possible avec, au minimum, des représentants de l'autorité communale, un responsable de la communication et un responsable informatique.
5. **S'appuyer sur un prestataire spécialisé** en *Incident Response*, qui pourra vous aider dans la gestion technique de l'incident en cybersécurité. La collecte de preuves, via les journaux de connexions (logs) de vos équipements, sera une des premières étapes techniques effectuées afin de comprendre l'attaque et son ampleur.
6. **Annoncer l'incident auprès de la Confédération** (NCSC / GovCERT) via le site https://www.report.ncsc.admin.ch/fr/

Canton de Vaud | Direction générale du numérique et des systèmes d'information (DGNSI)

Prenez en main votre sécurité informatique, utilisez ce QR code et suivez gratuitement une formation en ligne.

Pour les professionnels, rendez-vous sur : www.vd.ch/cybersecurite/

Merci de votre attention

Alexandre Herzog
NCSC.ch