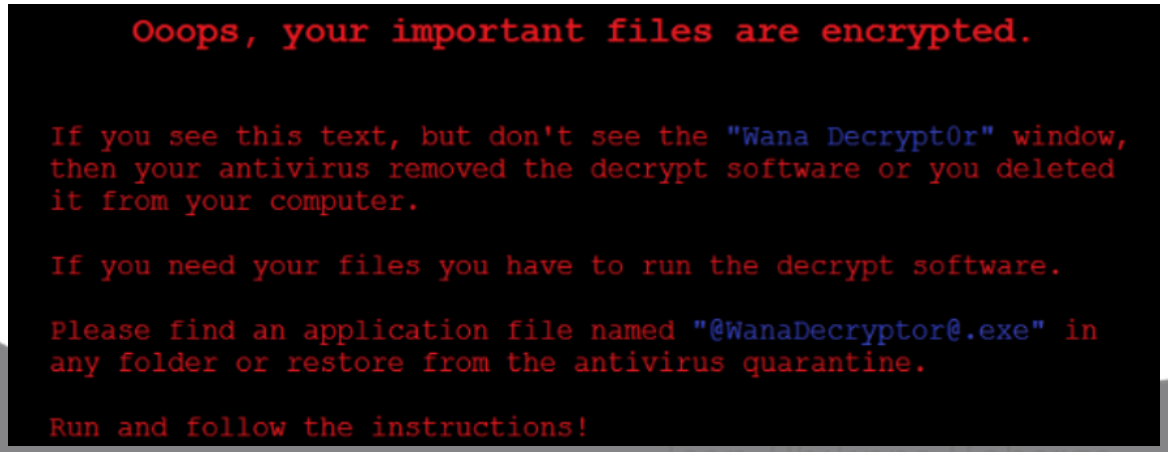
Wannacry (?)

Autres noms: *Wanna, WCry, Wannacrypt, Wannacrypt0r, Wanna Decryptor…*

- Pourquoi tout le monde en parle?
- D'où est-ce que ça provient?
- Qu'est-ce que c'est?
- Comment ça fonctionne?

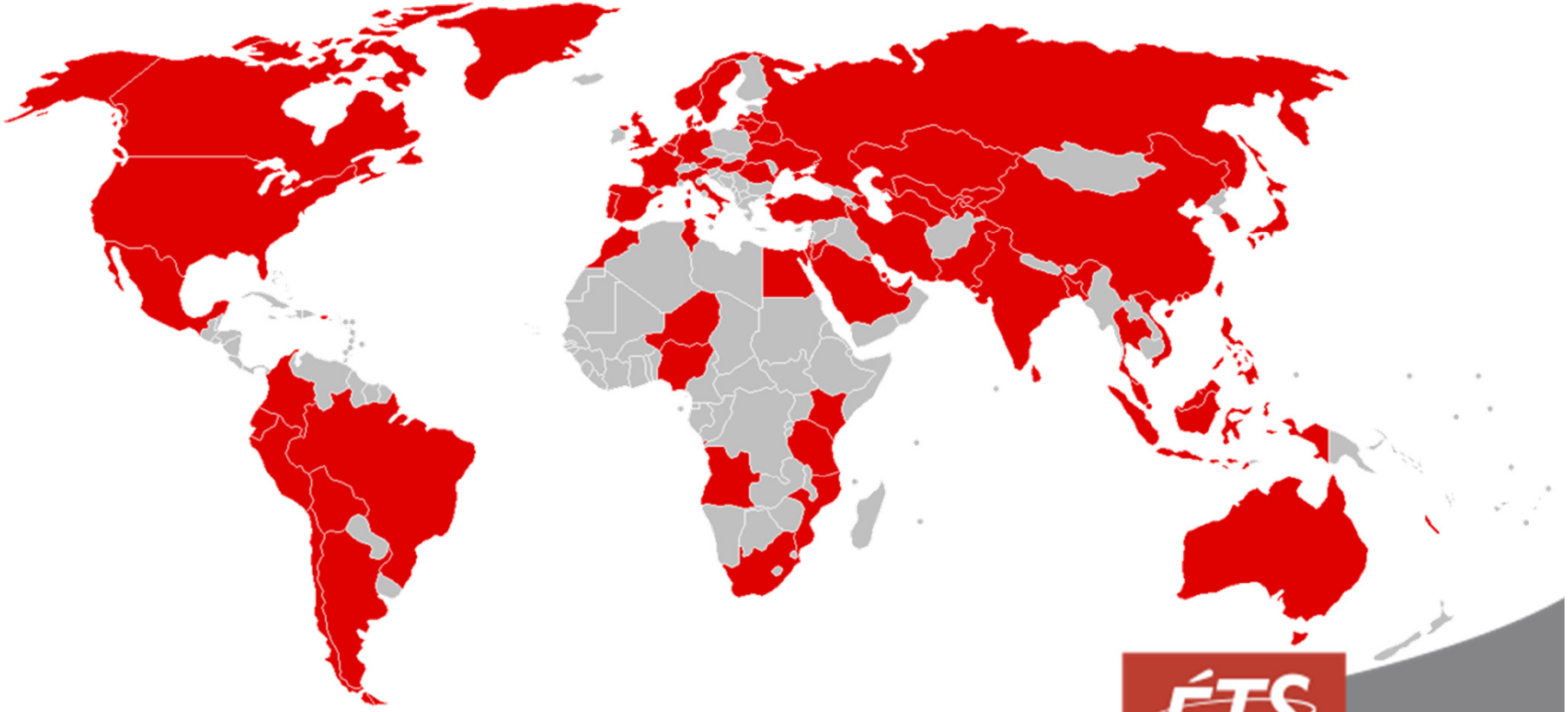


ÉTS Le génie pour l'industrie

Wannacry (1)

[Pourquoi tout le monde en parle?]

- En moins de 24 heures suivant l'attaque, un nombre estimé à 230 000 entitées dans plus de 150 pays sont affectées.

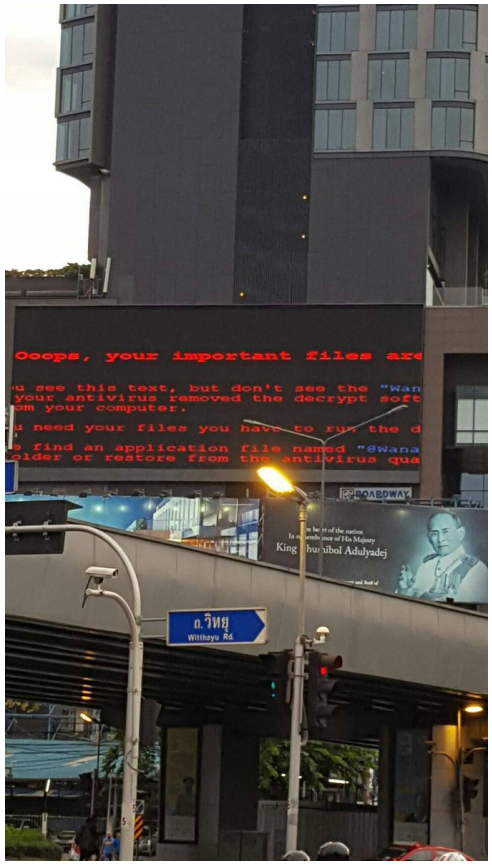


ÉTS
Le génie pour l'industrie

Wannacry (2)

[Pourquoi tout le monde en parle?]

- Plusieurs organisations majeures sont affectées par l'attaque d'envergure internationale:
  - Renault : forcé d'arrêter temporairement la production de voitures et ce, à plusieurs sites de fabrication en France.
  - FedEx
  - Bank of China: perte de plusieurs ATMs
  - Telefonica
  - Deutsche Bahn: les trains ont continué à fonctionner, mais les affichages des horaires non.
  - Nissan
  - Russia Central Bank
  - Russian Railways
  - Russian Interior Ministry
  - Indian Police
  - NHS (National Health Service) et autres hôpitaux: annulation de rendez-vous, imagerie par résonnance magnétique, réfrigérateur pour le sang…
  - Universités…



Wannacry (3)

[Pourquoi tout le monde en parle?]

- Parce que considérée comme la plus grosse attaque informatique de tous les temps en termes de sévérité des conséquences par Europol.
- Parce que la NSA est indirectement impliquée.
- Parce qu'il se pourrait que la provenance de l'attaque soit un groupe organisé et/ou même un état.
- Parce que cela a une incidence politique, Russie VS États-Unis / Trump VS la Corée du Nord.
- Parce que des individus très médiatisés, reliés à la sécurité informatique, en parlent:
  - Julian Assange
  - Edward Snowden

Wannacry (4)

[D'où est-ce que ça provient?]

- Parlons un peu de la NSA (National Security Agency)

Wannacry (5)

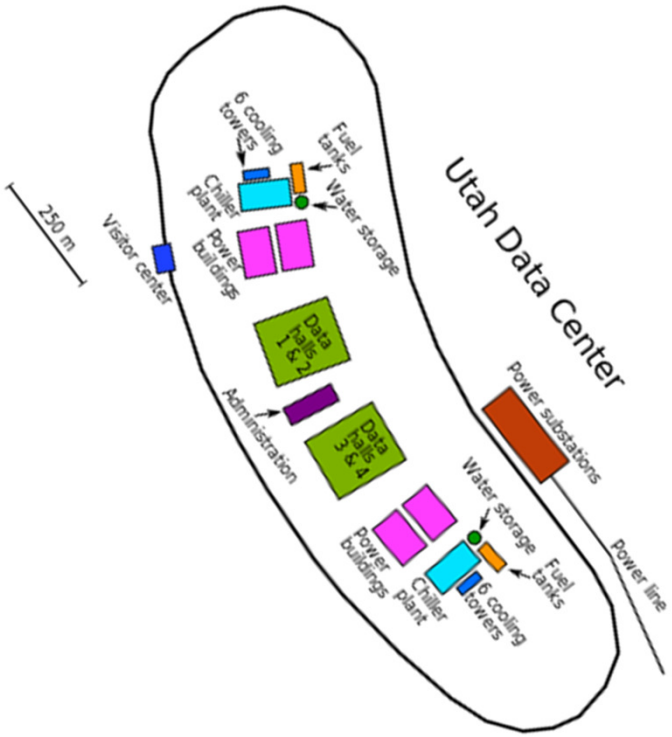
[D'où est-ce que ça provient?]

- Parlons un peu de la NSA (National Security Agency):
  - Fondée (confidentiellement) le 4 Novembre 1952
  - Nombre d'employés ≈ 30 000 – 40 000 (confidentiel, militaire + civils)
  - Budget ≈ 10.8 milliards US$ par année (en moyenne ces dernières années)
  - Requiert à elle seule une puissance de plus de 65 MegaWatts
  - Il s'agit d'une agence fédérale américaine chargée de la responsabilité de surveiller, recueillir, et d'analyser l'information et les données d'intelligence étrangère (pays étrangers), afin de constituer une puissance pouvant s'opposer à cette intelligence étrangère.
    - Une discpline appelée *signals intelligence* (SIGINT).

Wannacry (6)

[D'où est-ce que ça provient?]

- Parlons un peu de la NSA (National Security Agency):
  - Centre de données de l'Utah:



Le génie pour l'industrie

Wannacry (7)

[D'où est-ce que ça provient?]

- Elle engage une panoplie d'ingénieurs informatique, de programmeur, de scientifique de multiples horizons.
- Développe des algorithmes pour remplir sa mission, e.g.:
  - Collecte de données (controverses !)
  - Surveillance (controverses!)
  - Attaques (controverses!)
- *Notable Alumni:*
  - Edward Snowden - travaillait pour un contracteur de la NSA (Booz Allen Hamilton), mais travaillait physiquement dans les locaux. Très connu.
  - Harold T. Martin III - travaillait pour un contracteur de la NSA (Booz Allen Hamilton), mais travaillait physiquement dans les locaux. Moins connu..

ÉTS
Le génie pour l'industrie

Wannacry (8)

[D'où est-ce que ça provient?]

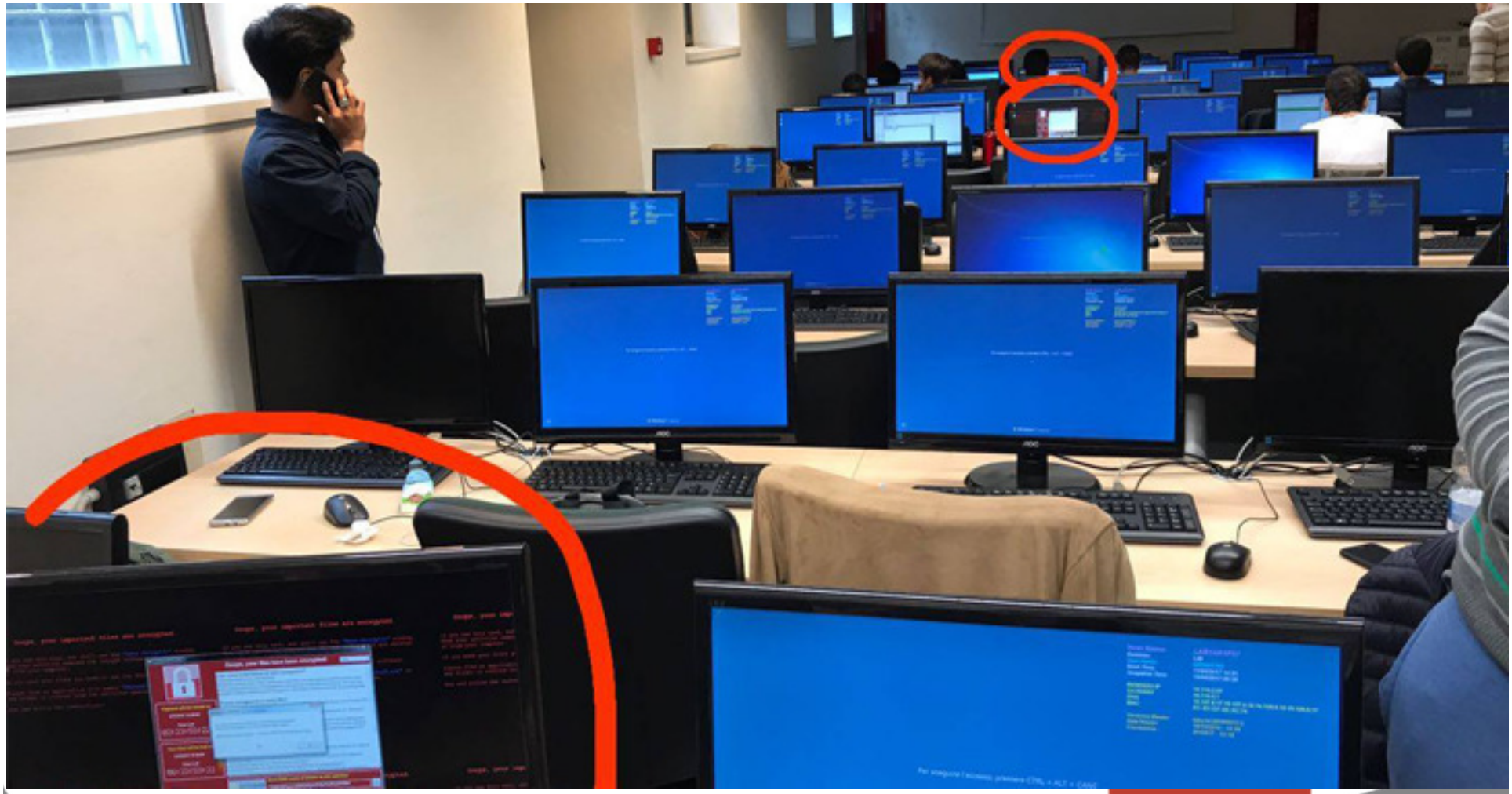
- **Edward Snowden**: Connu pour ses fuites d'information classifiées au site *wikileaks,* entres autres. Des films s'en sont même inspirés.
- **Harold T. Martin III**: Présentement enfermé, puisqu'accusé d'avoir volé environ 50 Tbytes de données confidentielles de la NSA.
  - **Accusé d'être à l'origine des fuites publicisées par le groupe de hackers *"The Shadow Brokers".***

Wannacry (9)

[D'où est-ce que ça provient?]

- **The Shadow Brokers:** Groupe de hackers apparu sur le web au cours de l'été 2016.
  - Publicisation de plusieurs fuites de la NSA:
    - *Leur hacking tools,* dont plusieurs *zero-day exploit*
  - Cinq publicisations:
    - 1 - "Equation Group Cyber Weapons Auction - Invitation"
    - 2 - "Message #5 - TrickOrTreat"
    - 3 - "Message #6 - BLACK FRIDAY / CYBER MONDAY SALE"
    - 4 - "Don't Forget Your Base"
    - 5 - "Lost in Translation" → **Eternal Blue exploit (14 avril 2017!)**

Wannacry (10)



Le génie pour l'industrie

Wannacry (11)

[Qu'est-ce que c'est?]

- *Wannacry* est un virus informatique de type "*worm"* et "*malware / ransomware"*
  - *Worm*: programme informatique indésirable auto-réplicant
  - *Malware:* programme malveillant
  - Ransomware: programme malveillant qui demande une rançon en échange d'un service
- Naissance: 12 mai 2017 (la semaine dernière!)
- Patch Windows XP (même si Windows avait annoncé qu'il y en aurait plus) en mars 2017
- Statut: toujours en vie, mais ralentit

Wannacry (12)

[Comment ça fonctionne ?]

- Infection initiale se fait de plusieurs façons possibles. Reportées:
  - Par courriel: *phishing emails*
  - Par insertion: Pdf, documents Words, exécutables…
  - Surtout, en exploitant une des vulnérabilités découvertes et utilisées par la NSA:
    - Eternal Blue → Protocole SMB (Simple balayage d'adresses IPs)
- Une fois infecté, un logiciel malveillant s'installe et encrypte une partie importante des fichiers utilisateurs.
- On demande alors une somme en bitcoin par dés-encrypter les fichiers.
- Simultanément, le logiciel scan tous les appareils attachés au réseau local et essaie de trouver les systèmes vulnérables (e.g. Windows XP non à jour) et tente de les infecter à leur tour

Wannacry (13)

[Comment ça fonctionne ?]

Le génie pour l'industrie

Wannacry (14)

[Comment ça fonctionne ?]

- Les bitcoins sont **partiellement non-traçables** et anonymes.
  - Dans ce cas, les hackers ont *hardcodé* (codé à la main) les porte-feuilles dans lesquels seraient versés les fonds extorqués, de sorte qu'il est possible de savoir combien d'argent a été envoyé jusqu'à maintenant:
    - https://twitter.com/ransomtracker
  - Par contre, dans ce cas particulier, vu l'ampleur de la chose, les états et administration suivent les fonds attentivement.
    - Leur conversion en devise sera fort probablement détectée et suivie.
    - → Donc pourquoi???

Wannacry (15)

- **Pourquoi**? Hypothèses avancées jusqu'à présent reportées dans différents médias:
  - Hackers du dimanche (vraiment?)
  - État derrière l'attaque. ?
    - États-Unis?
    - Russie?
    - Corée du Nord?
    - Chine?
  - Groupe organisé avec revendications:
    - Semer le chaos cybernétique pour manifester contre les politiques de Trump?
    - Réflexion par confrontation : réaliser les lacunes en sécurité informatiques.
    - Cyber-terrorisme?