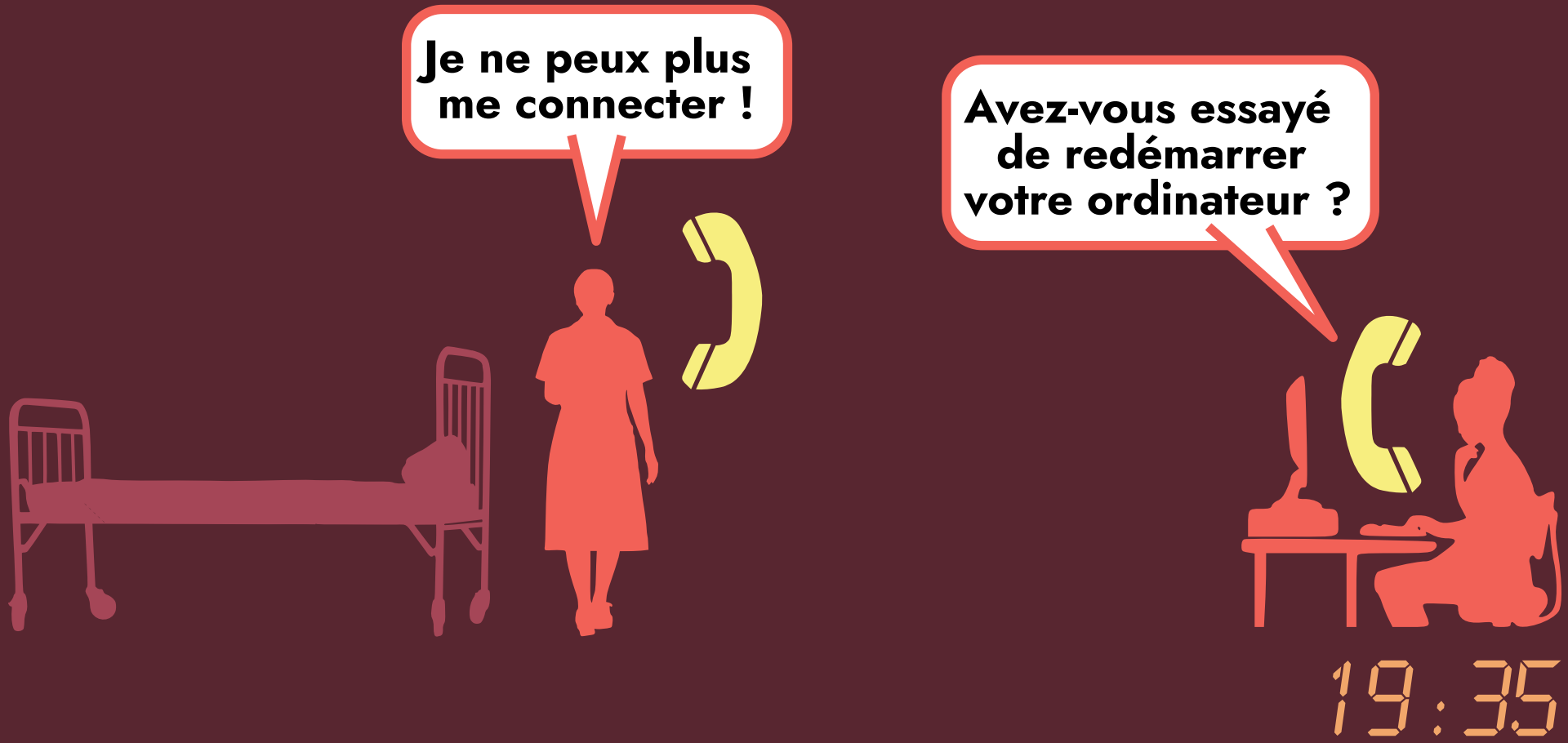
Cyberattaque au CHU de Rouen

Vendredi 15 novembre 2019

Une veille de week-end

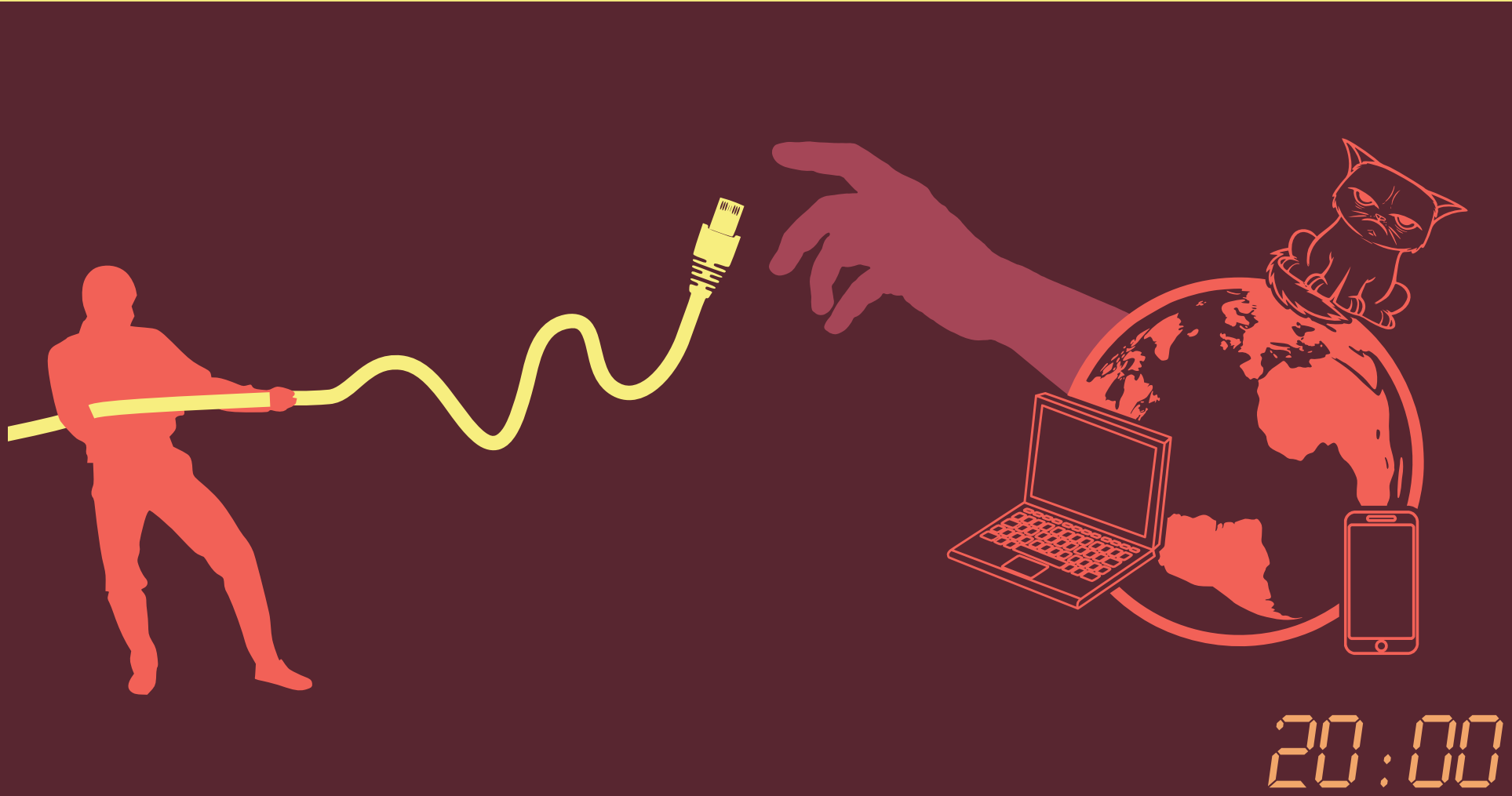
Ça ne marche pas !



Escalade de la hotline à la technique

Attaque détectée

Coupure d'internet

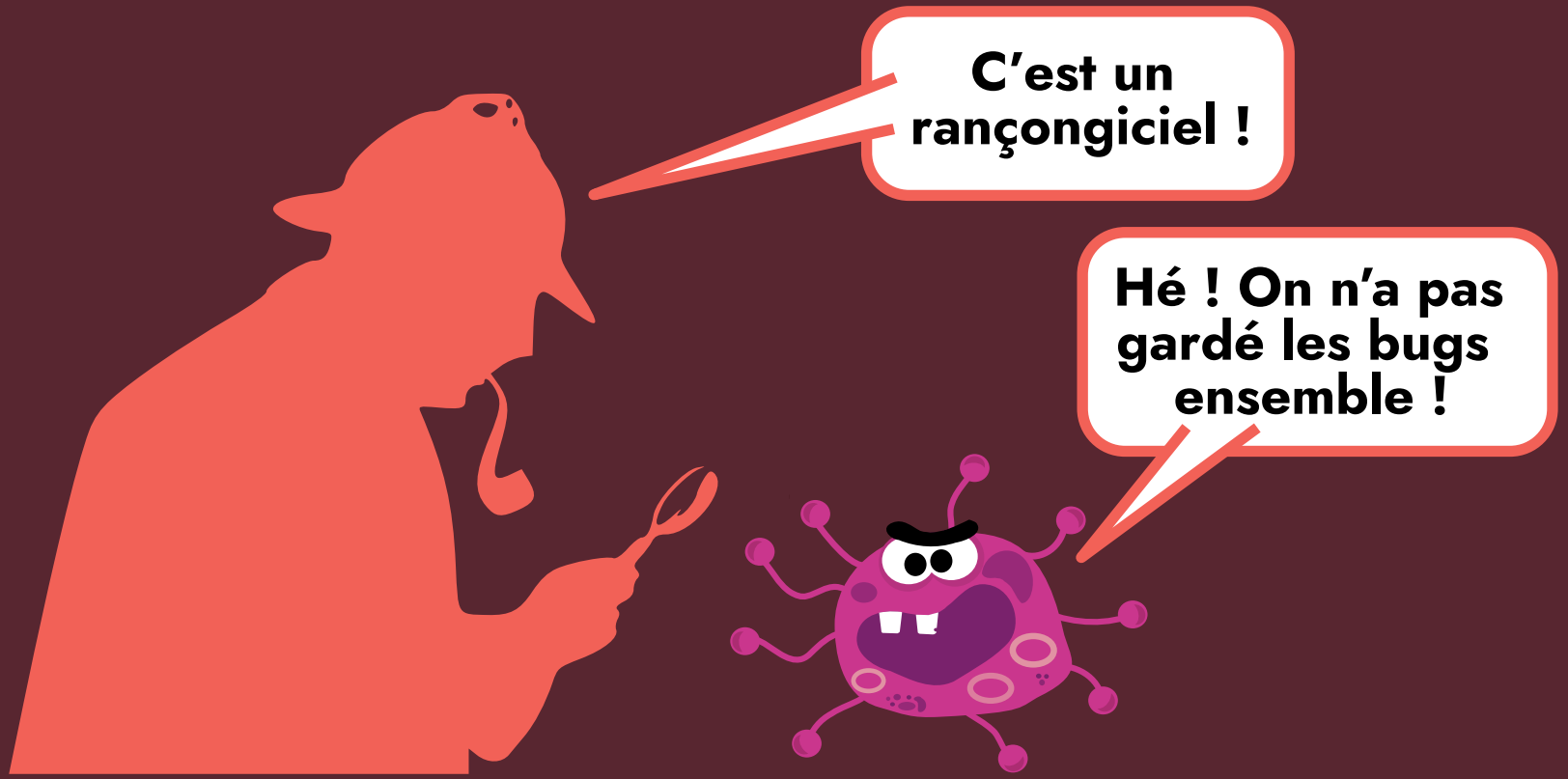


Ouverture d'une cellule de crise

Paris, nous avons un problème

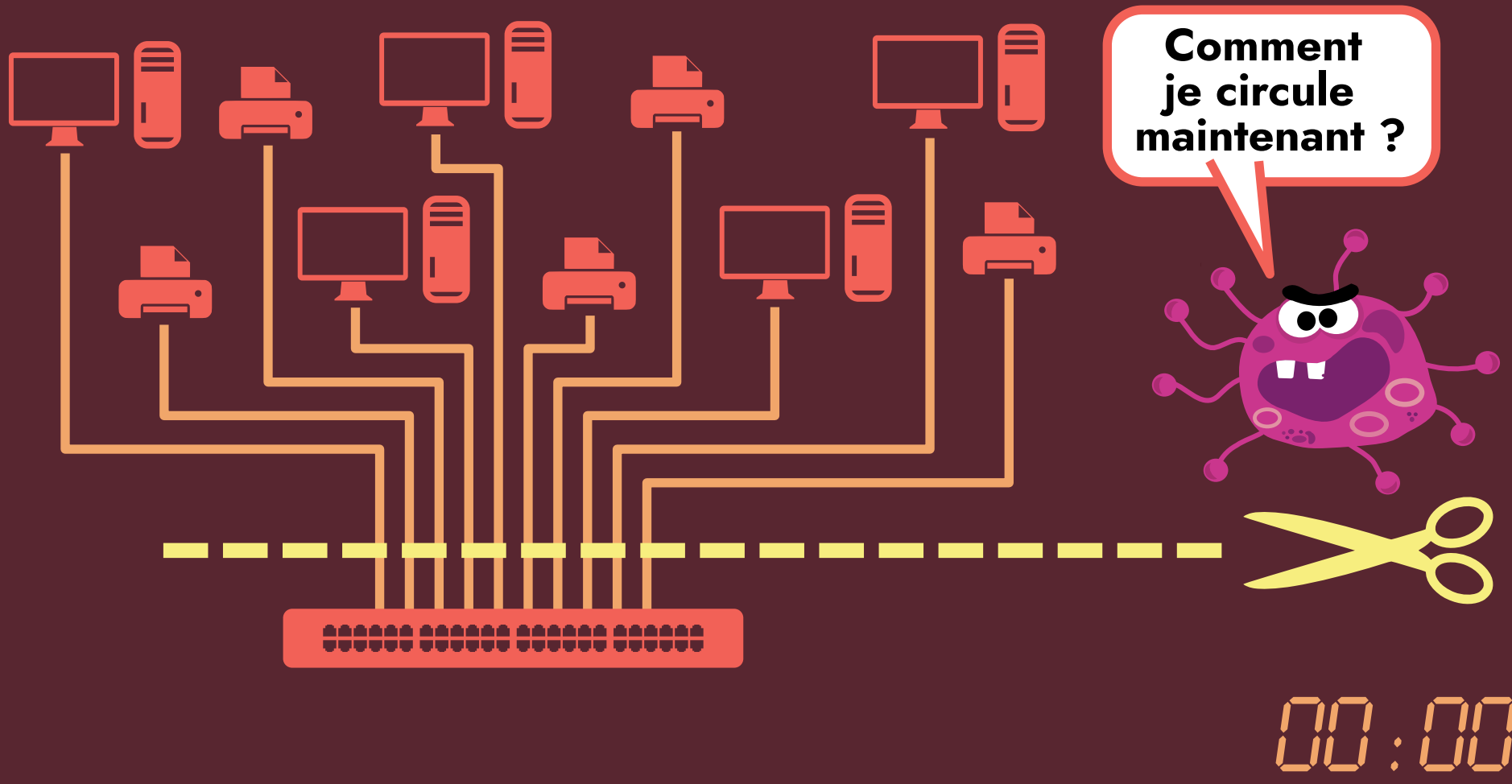
21 : 30

Attaque identifiée



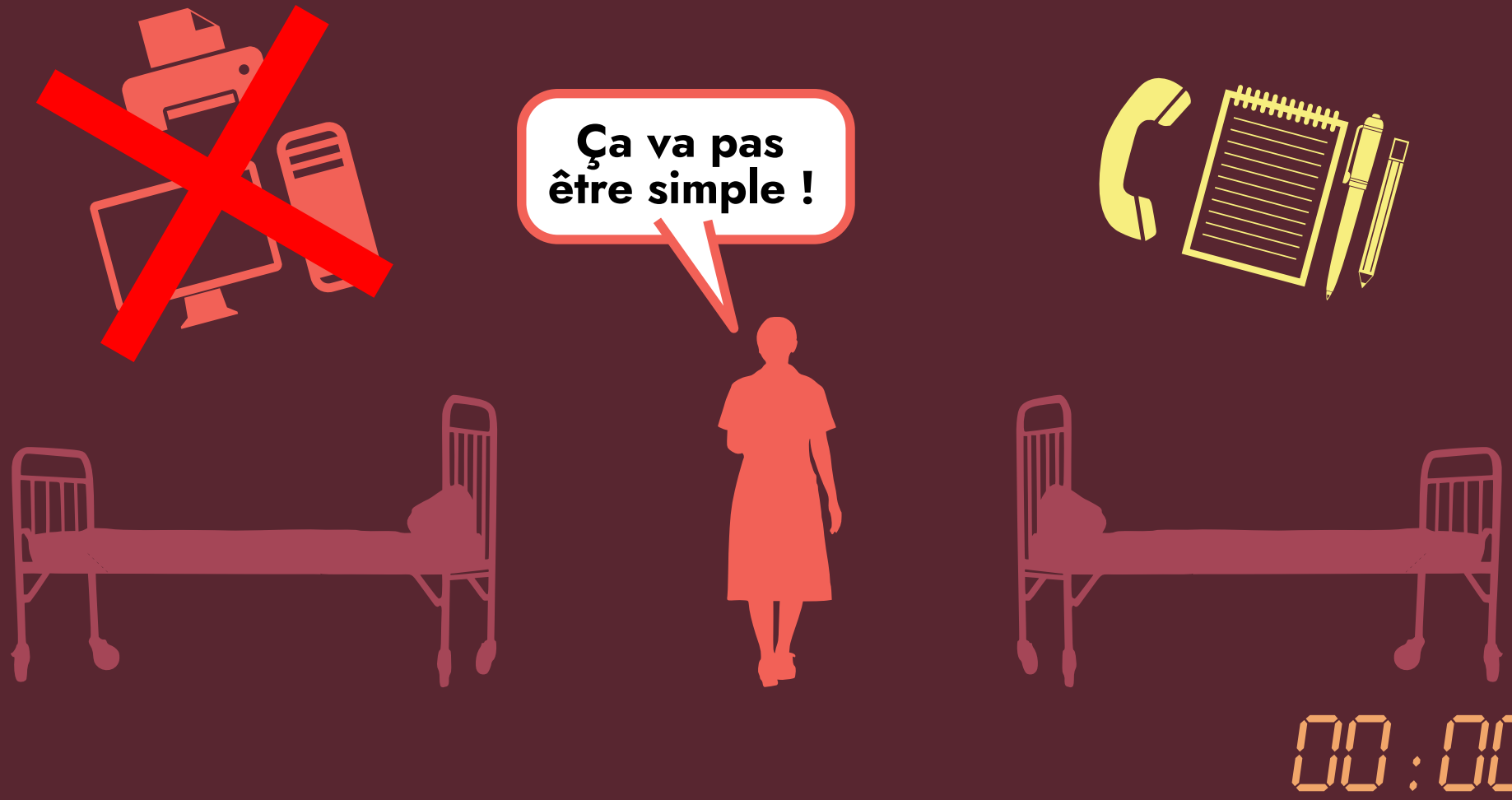
Déploiement d'agents sur le terrain

Coupure de tout le réseau !



Des renforts supplémentaires

Back to the paper



Les jours suivants, la DSI est sur le pont

- **samedi** : priorité aux services critiques
  agents en coordination sur le terrain
- **dimanche** : services critiques a minima
- **lundi** : services administratifs
  ouverture d'une enquête
- **mardi** : 60~70% des applications restaurées
  pas d'internet sur les postes de travail

10 jours plus tard, toujours pas d'internet

plus de lolcat,
de YouTube,
de Facebook…

plus d'intrusion !

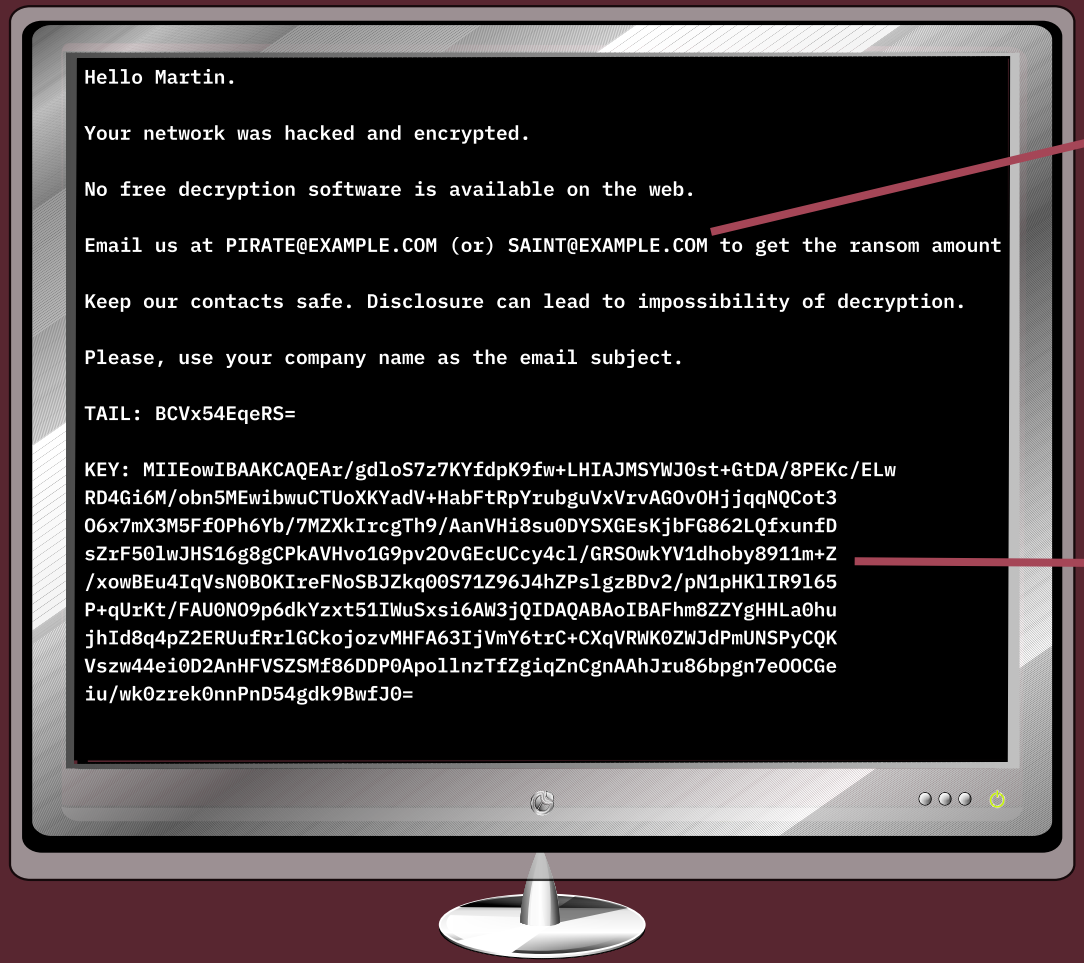
mais aussi plus
de SaaS, PaaS…

Un rançongiciel

Rançongiciel, ransomware, cryptolocker…

- **Il chiffre vos fichiers**
  avec un chiffrement asymétrique très costaud
- **Vous payez pour les déchiffrer**
  1 bitcoin par machine… à 7500 € le bitcoin en 11/19
- **Il se répand sur votre réseau**
  pour que les collègues en profitent
- **Les pirates communiquent à votre place**
  au cas où vous voudriez rester discrets

Il est trop tard quand vous lisez ceci



comment contacter
les pirates

clé unique
correspondant
à une machine

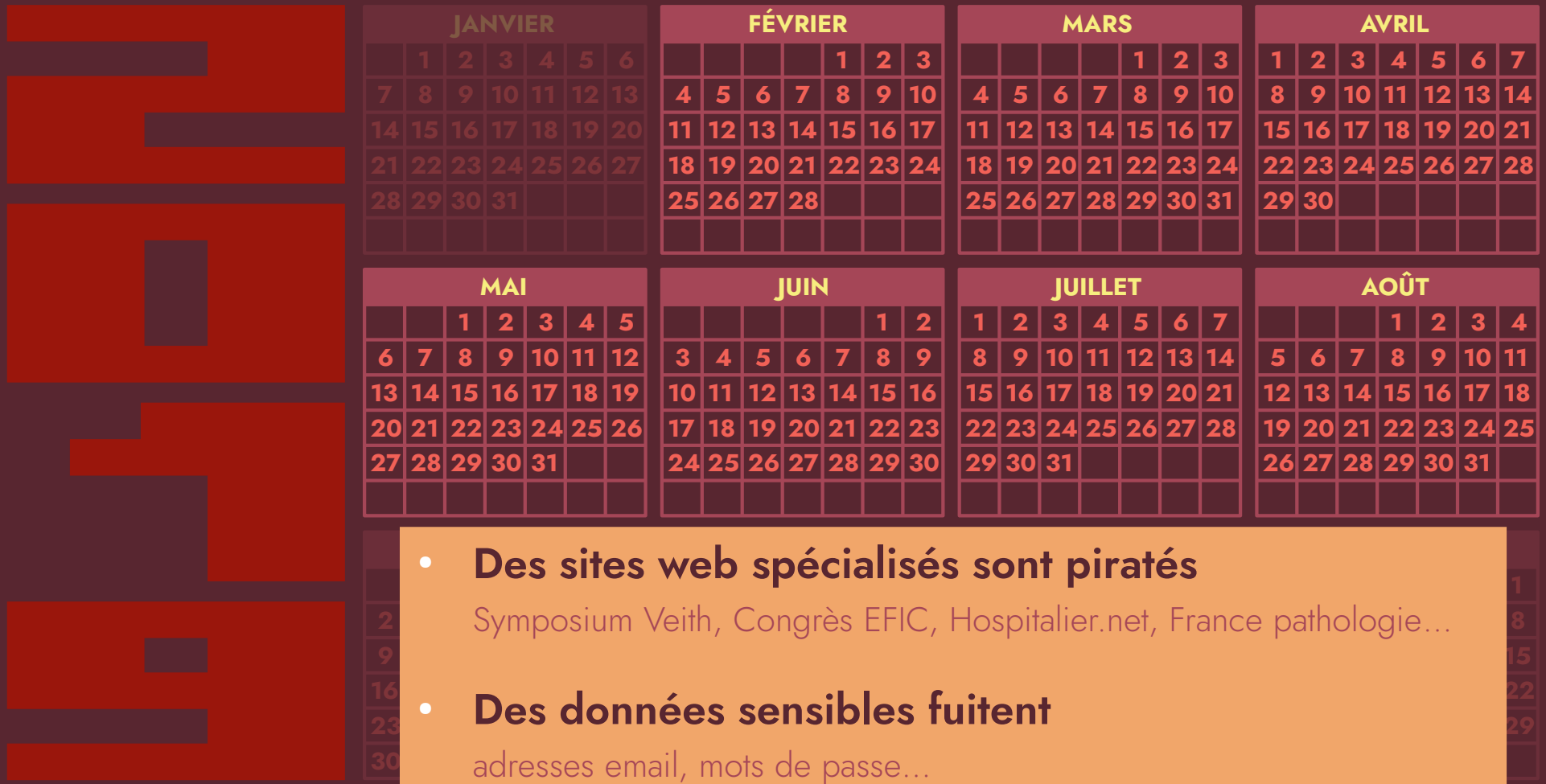
Où est la faille ?

- **Une pièce jointe dans un mail ?**
  hameçonnage / phishing
- **Un compte utilisateur sur le marché noir ?**
  mot de passe trop faible, utilisé plusieurs fois…
- **Une sécurité insuffisante ?**
  forte sécurité **vs** utilisation quotidienne

Une attaque se prépare

Février 2019

Avant septembre 2019



- **Des sites web spécialisés sont piratés**

  Symposium Veith, Congrès EFIC, Hospitalier.net, France pathologie…

- **Des données sensibles fuitent**

  adresses email, mots de passe…

De juin à novembre 2019

- **Forte activité de TA505**
  groupe russe ou russophone
  actif depuis 2014
- **9+ campagnes d'attaques**
  groupes financiers, hôpitaux…
- **PME de la cybercriminalité**
  oubliez le mythe du jeune génie isolé

aka SectorJ04 Group, GRACEFUL SPIDER, GOLD TAHOE…

7 septembre 2019

- **Un expert de Zataz alerte les autorités**
  Anssi, Cnil, Ministère des Affaires Sociales
- **Comptes vendus au marché noir**
  adresses email, mots de passe
- **CHU de Rouen concerné**

16 octobre 2019

- **Campagne d'hameçonnage**
  massive, non ciblée
- **Orchestrée par TA505**
- **Logiciel malveillant en pièce jointe**

Début novembre 2019

- **TA505 dans le réseau du CHU**
- **Phase de propagation manuelle**
  Clop ne sait pas se propager seul !
- **Utilisation de logiciels malveillants**
  ServHelper backdoor, FlawedAmmyy, Cobalt Strike
- **En toute discrétion…**

15 novembre 2019

- **À une heure propice**
  en début de soirée, la veille d'un week-end
- **TA505 lance le chiffrement**
- **Les applis métiers ne répondent plus**
- **Vous connaissez la suite !**

Quels sont les bons gestes ?

Ce qui a sauvé le CHU

- **Sauvegardes**
  elles ont permis de ne perdre aucune donnée
- **Incapacité du malware à se propager seul**
- **Hétérogénéité du SI**
  le malware préférait Windows
- **Réactivité du service informatique**
- **Cloisonnement du réseau, postes éteints**
  a limité la propagation du rançongiciel

Bons gestes 1/2

- **Méfiez-vous des mails**
  - du nom de l'expéditeur
  - des pièces jointes
  - des demandes d'infos confidentielles
  - des liens
- **Ne partagez pas votre carnet d'adresses**
- **Votre compte pro doit rester pro**

Bons gestes 2/2

- Éteignez votre ordinateur
- N'introduisez pas d'éléments extérieurs
  - pas de PC **perso** sur un réseau **pro**
  - pas de clé **perso** ou trouvée par terre
  - pas d'appli **perso** sur le téléphone **pro**
- Ne prêtez pas votre matériel **pro**
- Et n'oubliez jamais que…

N’oubliez jamais que...

PERSONNE N’EST À L’ABRI

Un doute ?

UN MAIL SUSPECT ?
UNE ALERTE SÉCURITÉ ?
UN PC BLOQUÉ ?

QUI APPELLE-T-ON ?

APPELEZ VOTRE DSI