MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Évolutions des rançongiciels

Général **Éric FREYSSINET**, docteur en informatique

Séminaire sur les Écosystèmes cybercriminels, Campus Cyber, 12/03/2025

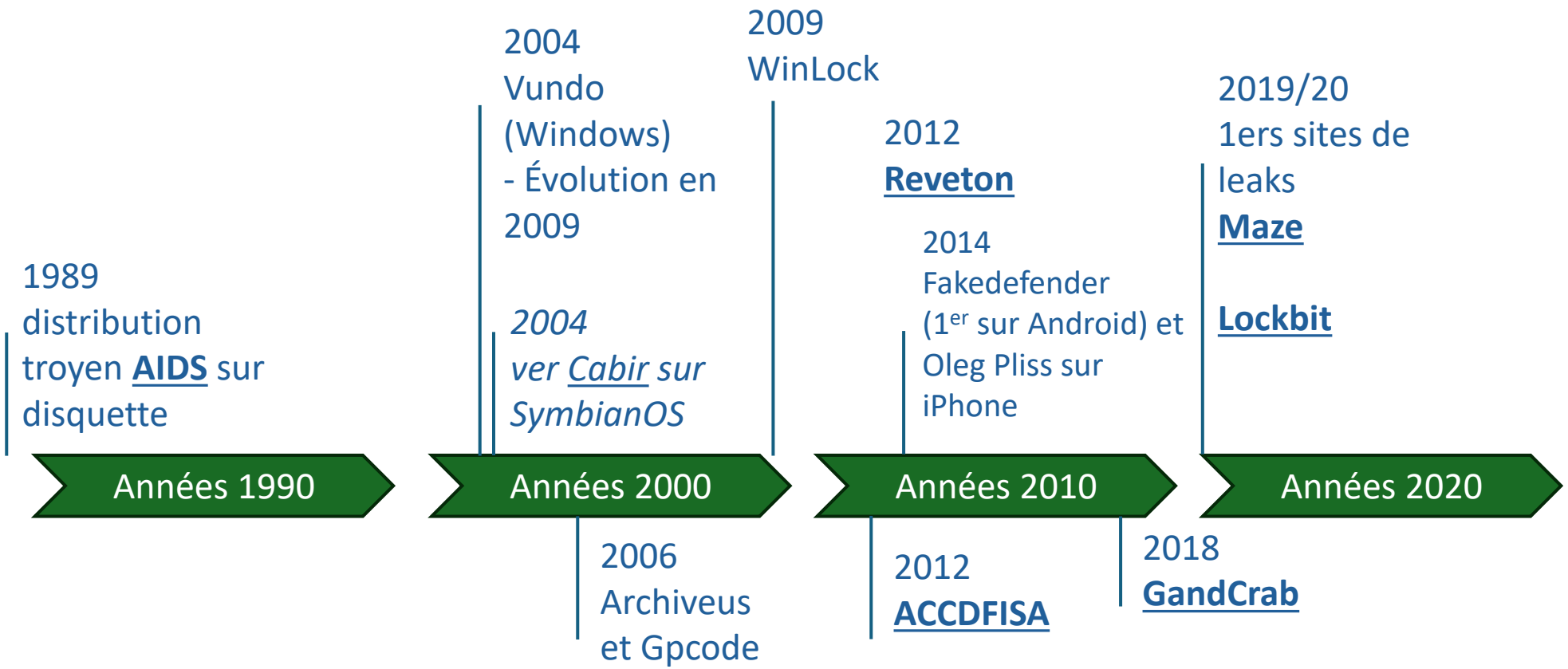
PROJET DEFMAL
Défense contre les programmes malveillants

FRANCE 2030 PROGRAMME DE RECHERCHE CYBERSÉCURITÉ

TLP:WHITE

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

HISTORIQUE DES RANÇONGICIELS (QUELQUES DATES)

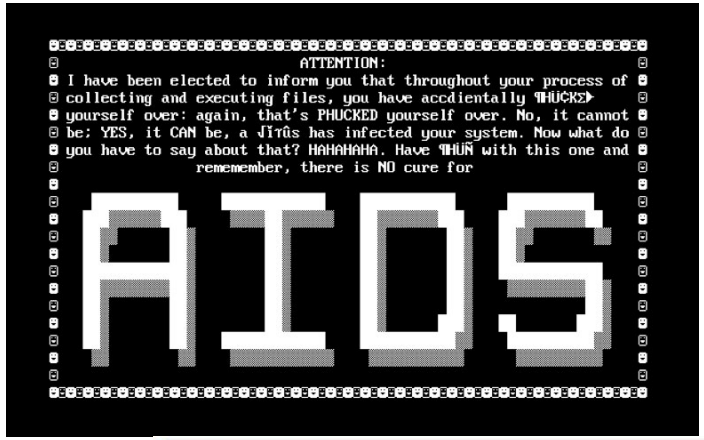


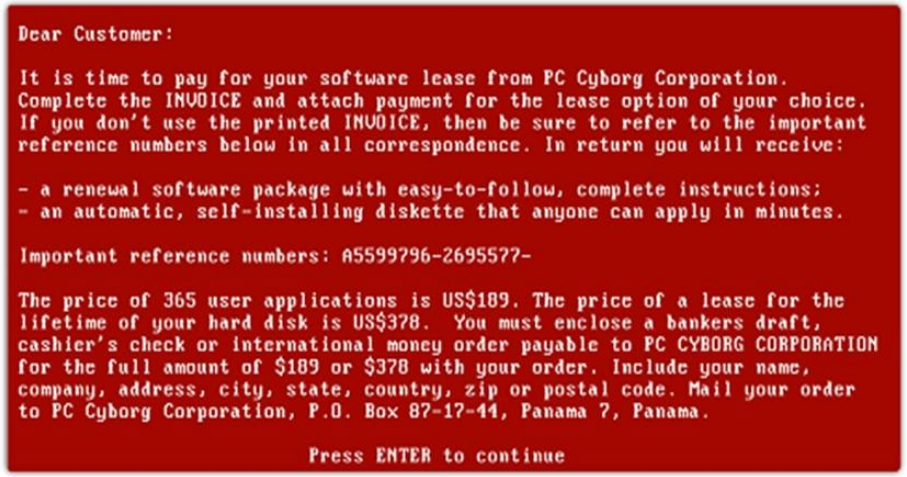
loria Laboratoire lorrain de recherche en informatique et ses applications

COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

L'ANCÊTRE - AIDS





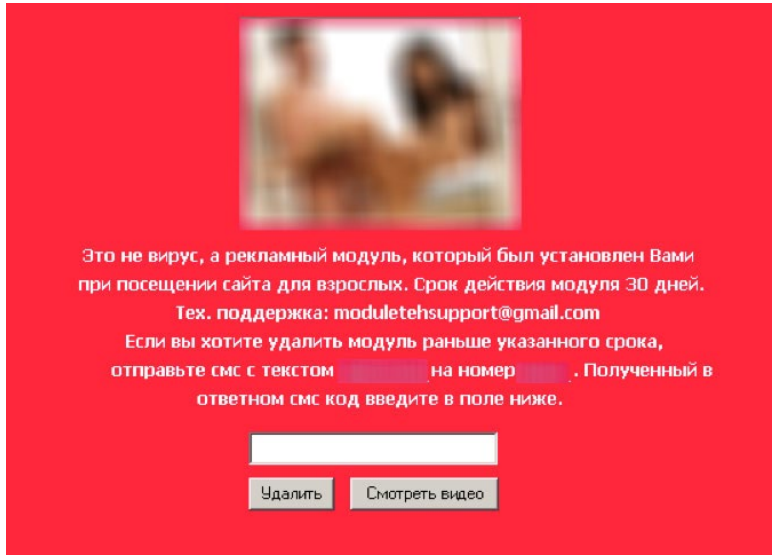
- Développé par un biologiste américain, distribué sur 20.000 disquettes à une conférence de l'OMS en 1989
- Le PC redémarre 90 fois, le nom des fichiers est chiffré
- $189 à envoyer à une boîte postale au Panama

loria Laboratoire lorrain de recherche en informatique et ses applications
COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

PREMIERS RANÇONCIGIELS SUR PC, AVANT TOUT DES « LOCKERS »

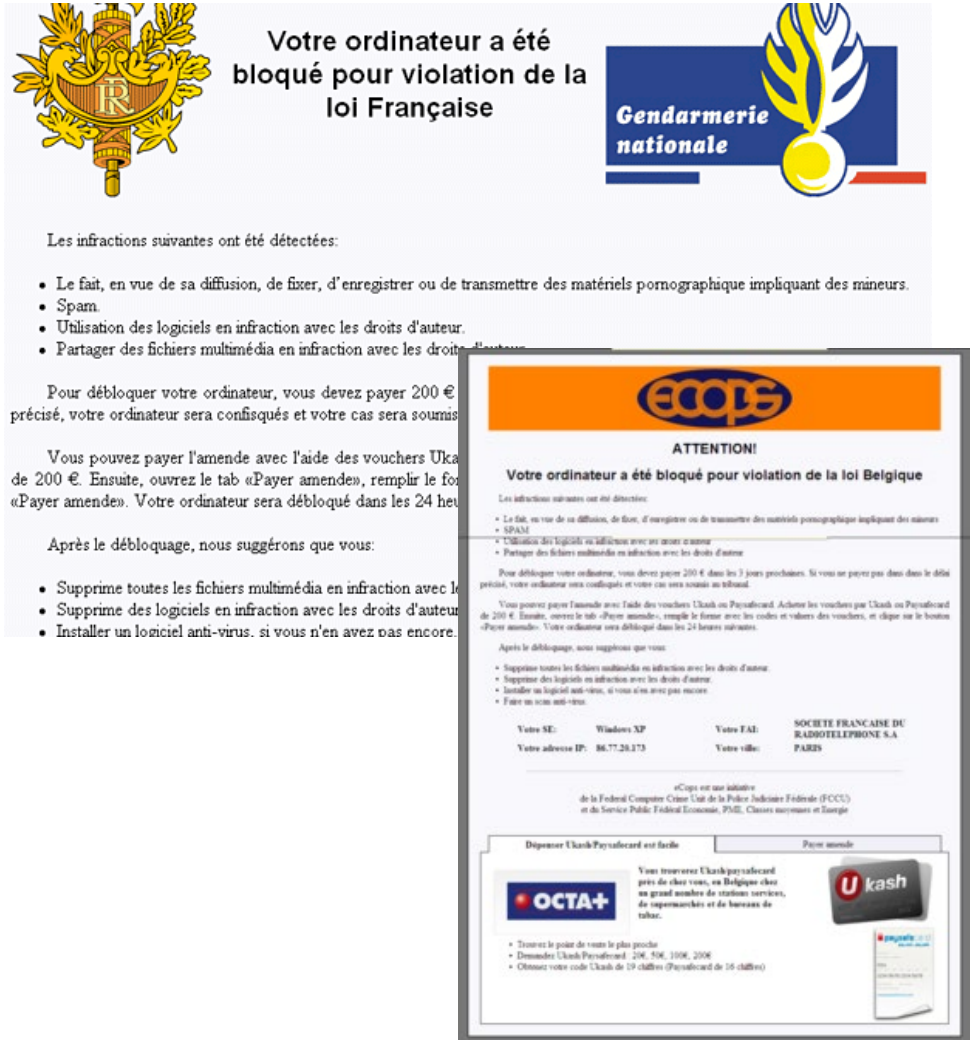
- Vundo
  - Par courrier électronique en pièce jointe
  - Par exploits sur navigateur Web
  - Bloque l'utilisation normale de l'ordinateur
  - A évolué ensuite en rançongiciel chiffrant
- Winlock
  - Bloque l'écran par l'affichage de pornographie jusqu'à ce qu'on paye par SMS surtaxé
  - Diffusion par d'autres logiciels malveillants
  - Cible des utilisateurs russes



loria Laboratoire lorrain de recherche en informatique et ses applications
COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

REVETON (ET AL.) – LE PASSAGE À L'ÉCHELLE MONDIALE

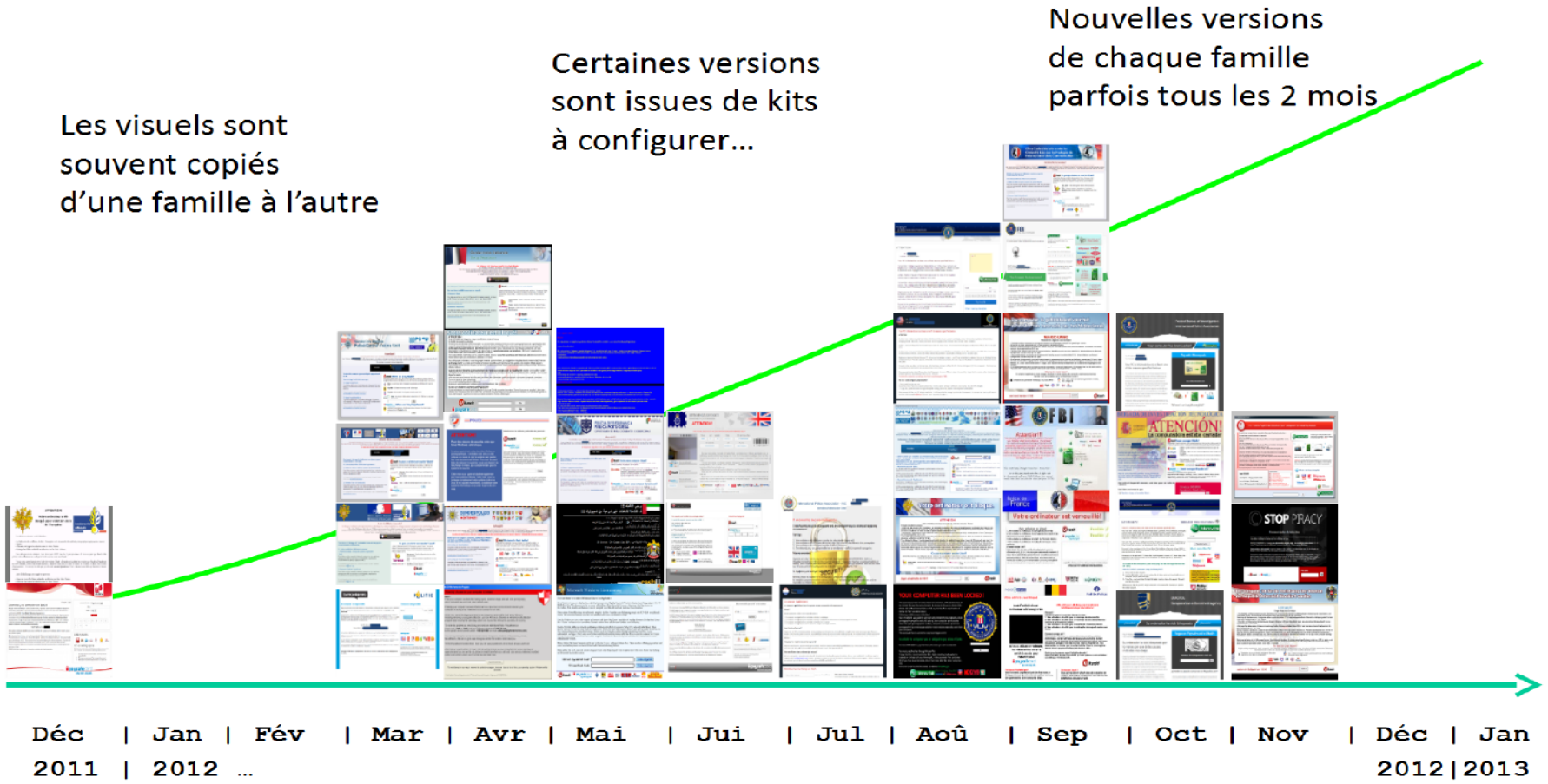


- 2011-2012
- Diffusion par « drive-by download » (souvent via des bannières publicitaires ou des sites Web modifiés)
- Une page Web s'affiche et empêche l'utilisation de l'ordinateur
- Uniquement dans le navigateur (« weblocker ») ou logiciel malveillant plus complet
- Les rançons sont à payer en tickets Paysafecard et autres systèmes prépayés

loria Laboratoire lorrain de recherche en informatique et ses applications
COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

PAGES D'ACCUEIL (« LANDING PAGE ») DES RANÇONGICIELS EN 2012



Source: E. Freyssinet, Lutte contre les botnets

loria Laboratoire lorrain de recherche en informatique et ses applications

COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

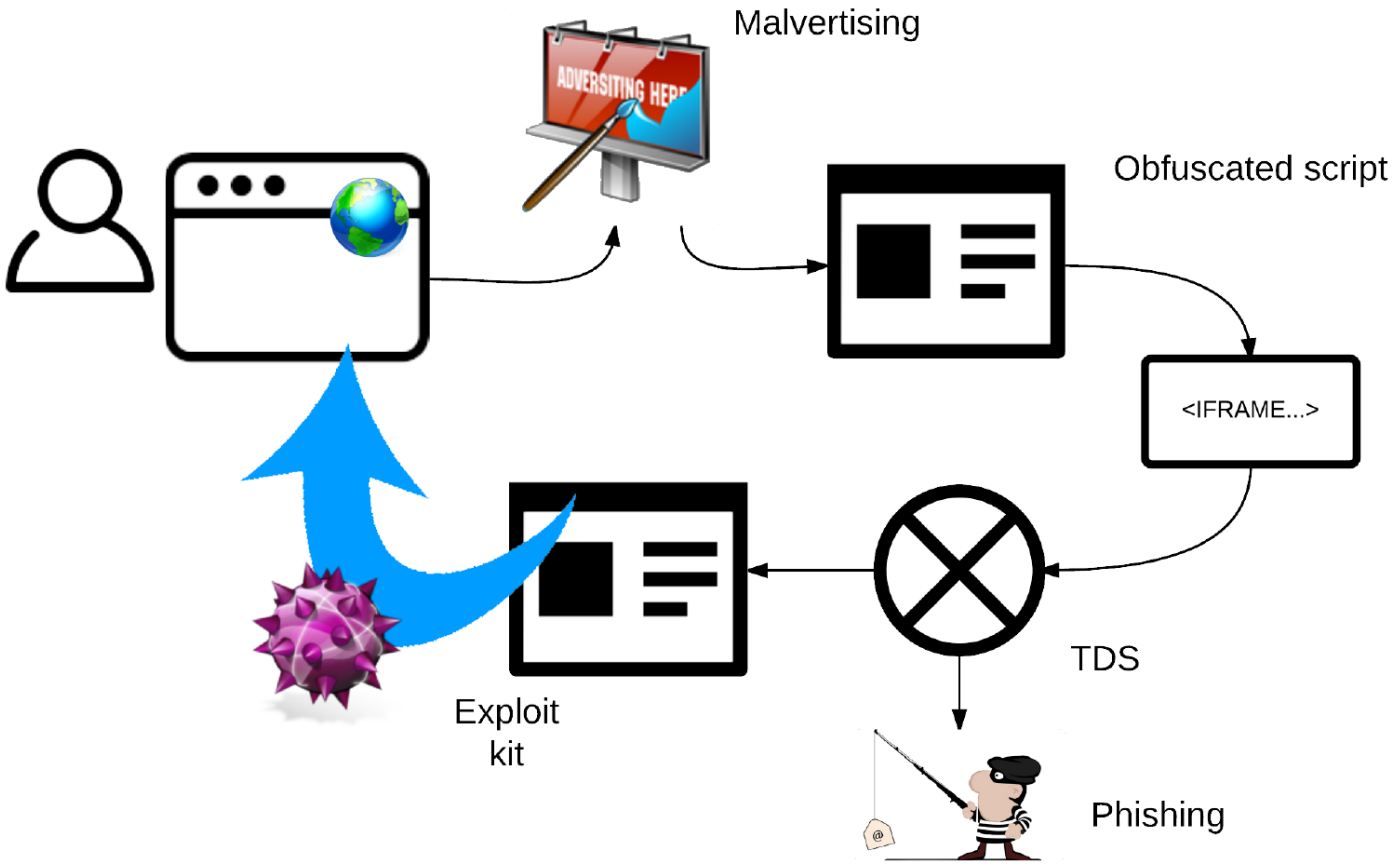
CRYPTOLOCKER – L'AVÈNEMENT DES RANÇONGICIELS CHIFFRANTS

- 2013
- Diffusion par GameOver ZeuS (troyen bancaire)
- Chiffrement RSA 2048 bits

loria
COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

SCHÉMA TYPE DE DISTRIBUTION DES LOCKERS PAR « MALVERTISING »

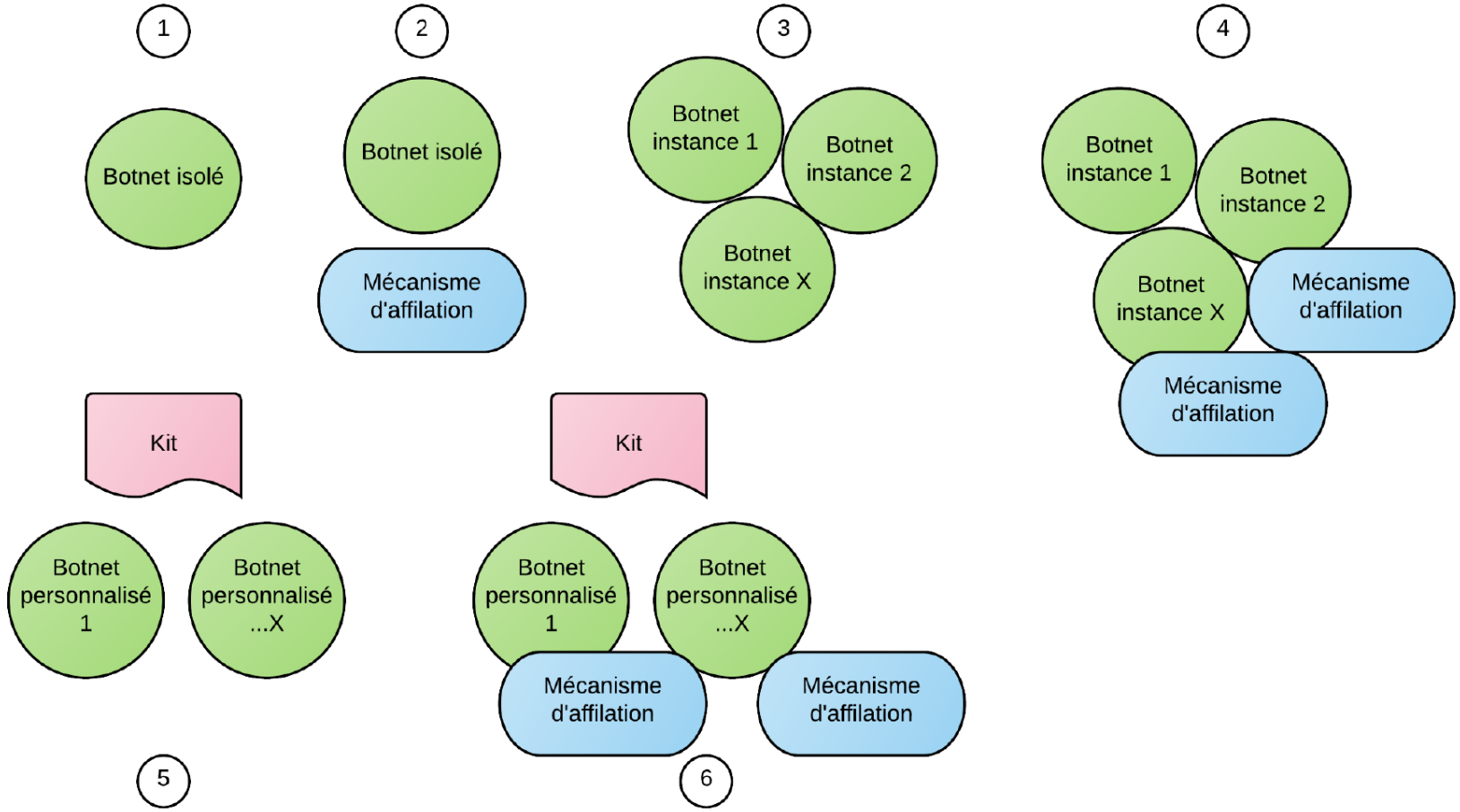


Source: E. Freyssinet, Lutte contre les botnets

loria
COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

DIFFÉRENTES ARCHITECTURES POSSIBLES



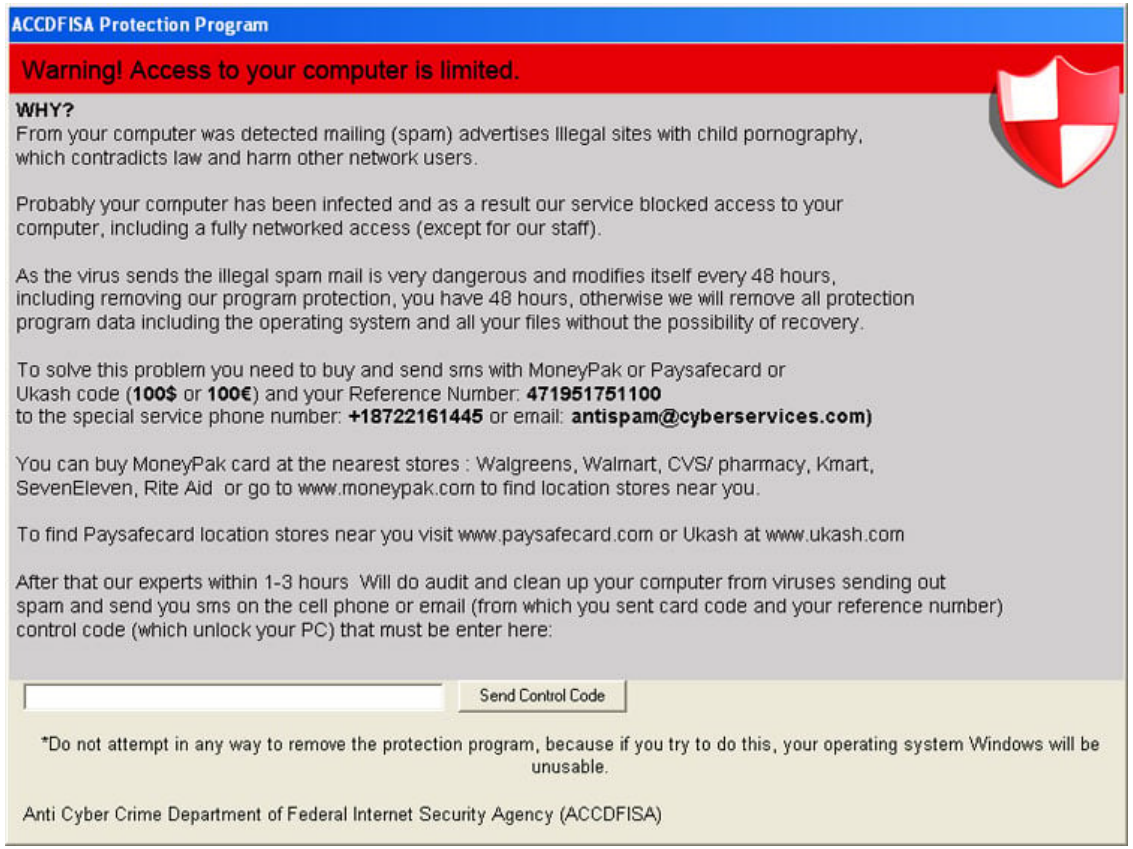
Source: E. Freyssinet, Lutte contre les botnets

loria Laboratoire lorrain de recherche en informatique et ses applications

COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ACCDFISA – CIBLAGE DES RÉSEAUX D'ENTREPRISE



- 2012
- Installation via vulnérabilités dans les services RDP d'accès à distance (remote desktop protocol), a priori ciblage manuel (notamment avec DUBrute)
- Vise plutôt des serveurs Windows
- Trois composantes:
  - Le screen locker
  - Le cryptogiciel lui-même
  - L'outil de déchiffrement (victime)

https://www.emsisoft.com/en/blog/818/the-accdfisa-malware-family-ransomware-targetting-windows-servers/

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

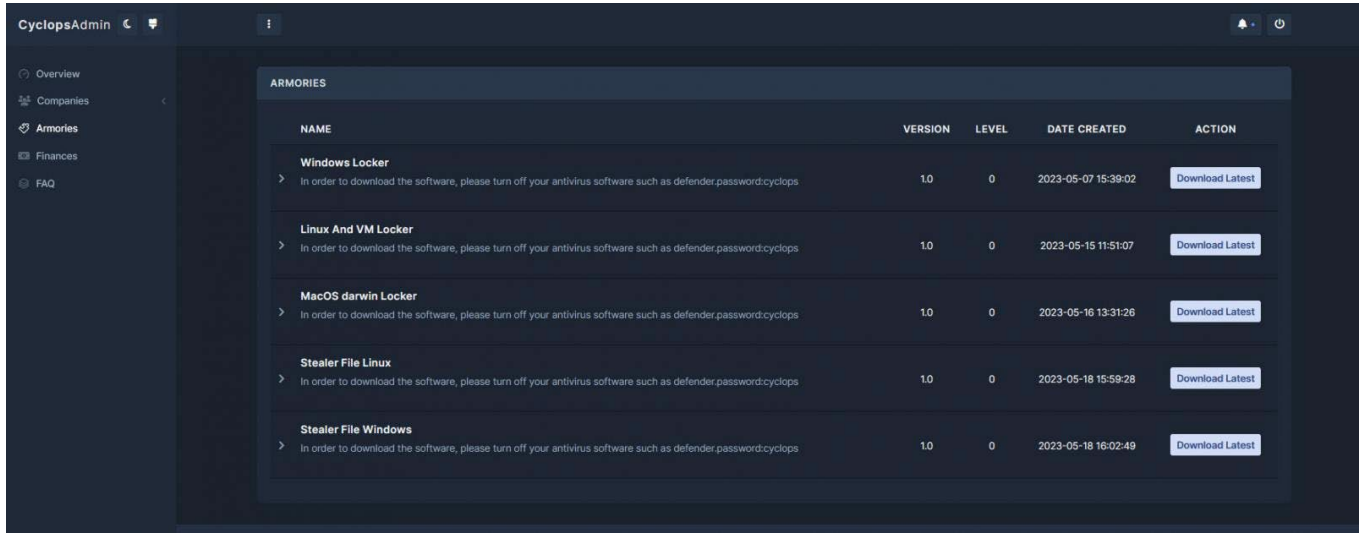
PREMIER BILAN

- Les rançongiciels (chiffrants) sont un des premiers exemples (avec les botnets bancaires notamment) de développement des écosystèmes cybercriminels autour des malware:
  - Développement (logiciel malveillant et de pilotage C&C)
  - Revente de kits plus ou moins complets
  - Affiliation (ceux qui vont infecter les cibles)
  - Blanchiment des données dérobées et de l'argent
- Pas de ciblage réel au cours des premières années (opportunisme), faibles montants individuels, début de ciblage de réseaux d'entreprises avec ACCDFISA

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

RANSOMWARE AS A SERVICE

- Emergence vers 2015
- Les différentes plateformes permettent de gérer un nombre de plus en plus grand d'affiliés (Revil, DarkSide, LockBit, Ransomhub…)
- En même temps, la stratégie évolue pour inclure le **détournement de données** qui devient petit à petit la monnaie d'échange principale



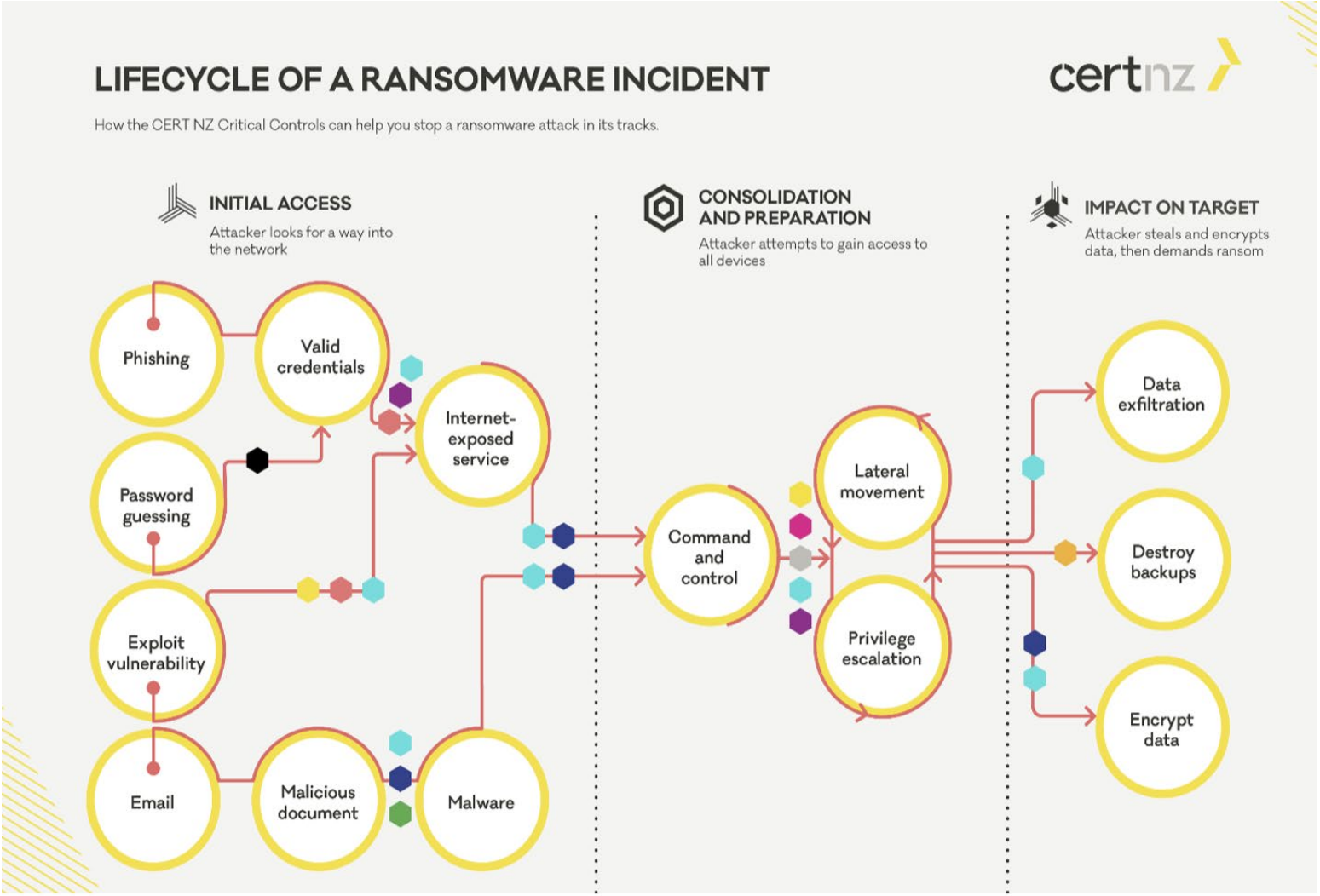
Ex. panel Cyclops de distribution de logiciels malveillants ciblant différentes plateformes (source Bleepingcomputer)

loria Laboratoire lorrain de recherche en informatique et ses applications

COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

CYCLE TYPIQUE DES RANÇONGICIELS AUJOURD'HUI



- Evolution vers le « big game hunting »
- Petit à petit le vol de données devient le cœur de la démarche, et de la menace. Plus le DDoS.
- Le montant des rançons s'adapte à la cible
- On devrait plus parler de **groupes cybercriminels rançonneurs** (ou extorqueurs)

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

HISTORIQUE DES RANÇONGICIELS

1989
distribution troyen **AIDS** sur disquette

2004
Vundo (Windows) - Évolution en 2009

2004
ver Cabir sur SymbianOS

2009
WinLock

2012
Reveton

2014
Fakedefender (1er sur Android) et Oleg Pliss sur iPhone

2019/20
1ers sites de leaks
Maze

Lockbit

Années 1990 | Années 2000 | Années 2010 | Années 2020

2006
Archiveus et Gpcode

2012
ACCDFISA

2018
GandCrab

Locker simple

Chiffrement

Vol de données

Ordinateurs individuels

Réseaux d'entreprises

loria Laboratoire lorrain de recherche en informatique et ses applications

COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

QUE RETENIR

- **En résumé**, le rançonnage cyber:
  - Dès les années 90
  - Explose au début des années 2010, introduit petit à petit le chiffrement
  - Cible parfois les téléphones mobiles
  - … et s'industrialise
  - A ciblé des victimes au hasard d'abord
  - … puis de façon beaucoup plus ciblée des particuliers vers les organisations
  - Est un exemple typique de développement d'un écosystème cybercriminel complet

- Comment ce phénomène pourra **évoluer** après ?
  - Retour vers un ciblage opportuniste ? PMEs et particuliers.
  - Rançonnage plus agressif et ciblé dans certains cas sur la base des données récupérées
- Les techniques tels que les mécanismes de distribution par la publicité malveillante existent toujours pour d'autres types de cybermalveillances (autres logiciels malveillants, escroquerie au faux support technique…)

loria Laboratoire lorrain de recherche en informatique et ses applications
COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

QUESTIONS

COMCYBER-MI