

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

Évolutions des rançongiciels

Général **Éric FREYSSINET**, docteur en informatique

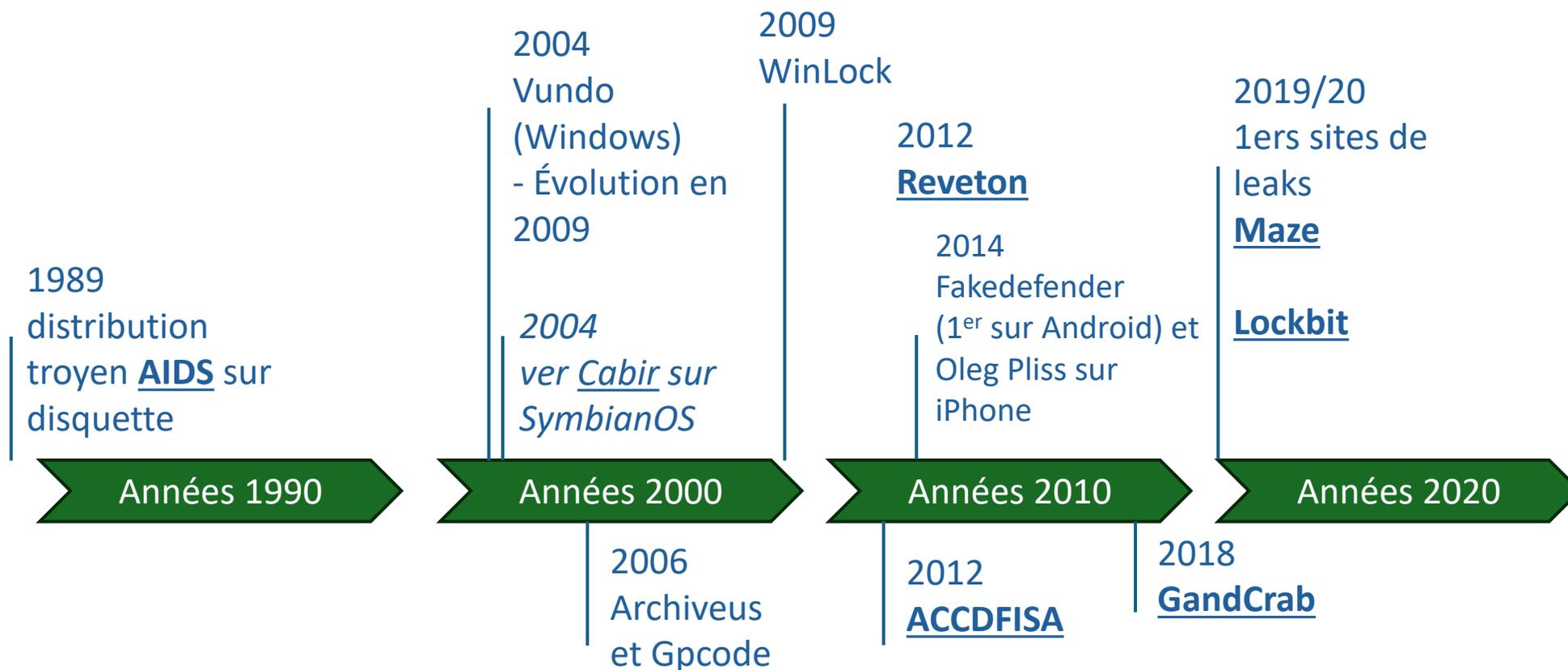
Séminaire sur les Écosystèmes cybercriminels, Campus Cyber, 12/03/2025

PROJET DEFMAL

Défense contre les programmes malveillants



HISTORIQUE DES RANÇONGIERS (QUELQUES DATES)



L'ANCÊTRE - AIDS



Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

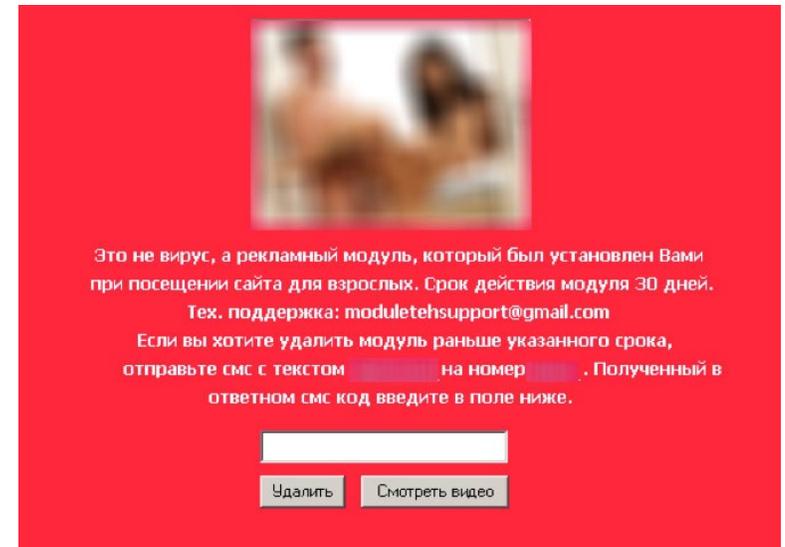
The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

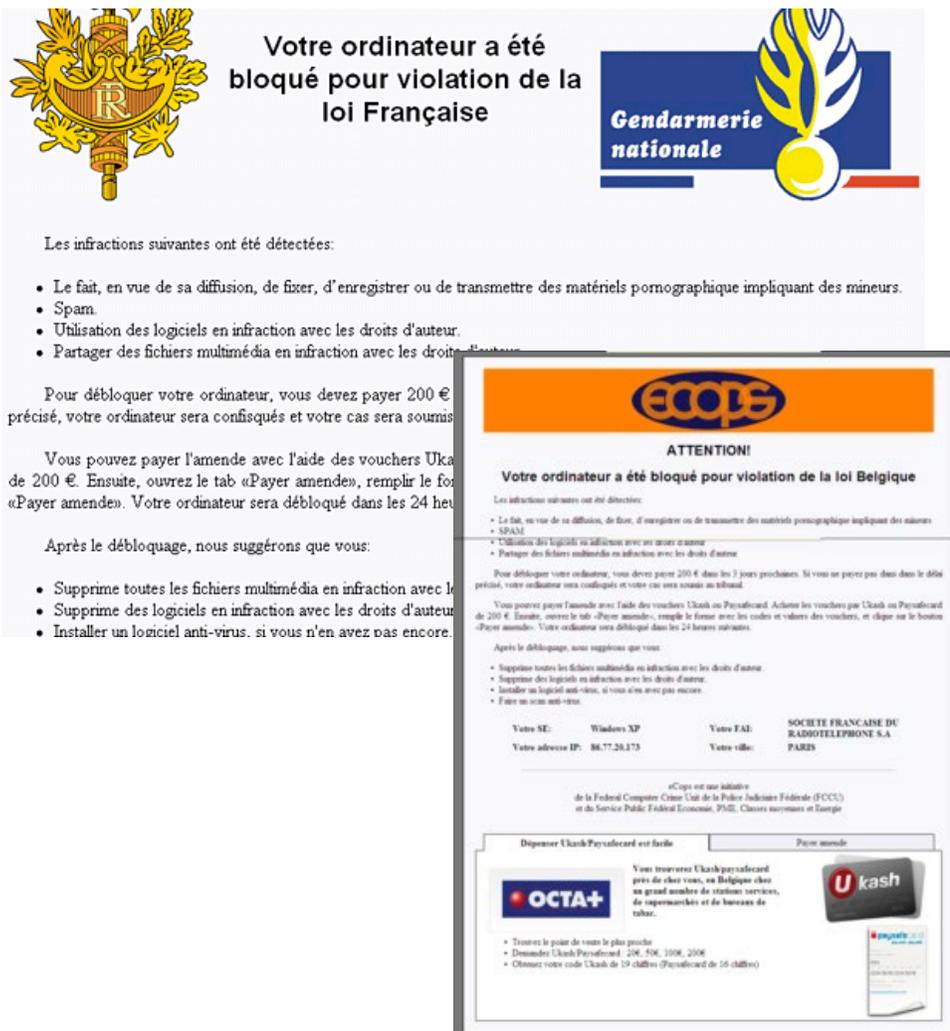
- Développé par un biologiste américain, distribué sur 20.000 disquettes à une conférence de l'OMS en 1989
- Le PC redémarre 90 fois, le nom des fichiers est chiffré
- \$189 à envoyer à une boîte postale au Panama

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



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



Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre des matériels pornographique impliquant des mineurs.

- Spam.
- Utilisation des logiciels en infraction avec les droits d'auteur.
- Partager des fichiers multimédia en infraction avec les droits d'auteur.

Pour débloquent votre ordinateur, vous devez payer 200 € précisée, votre ordinateur sera confisqués et votre cas sera soumis

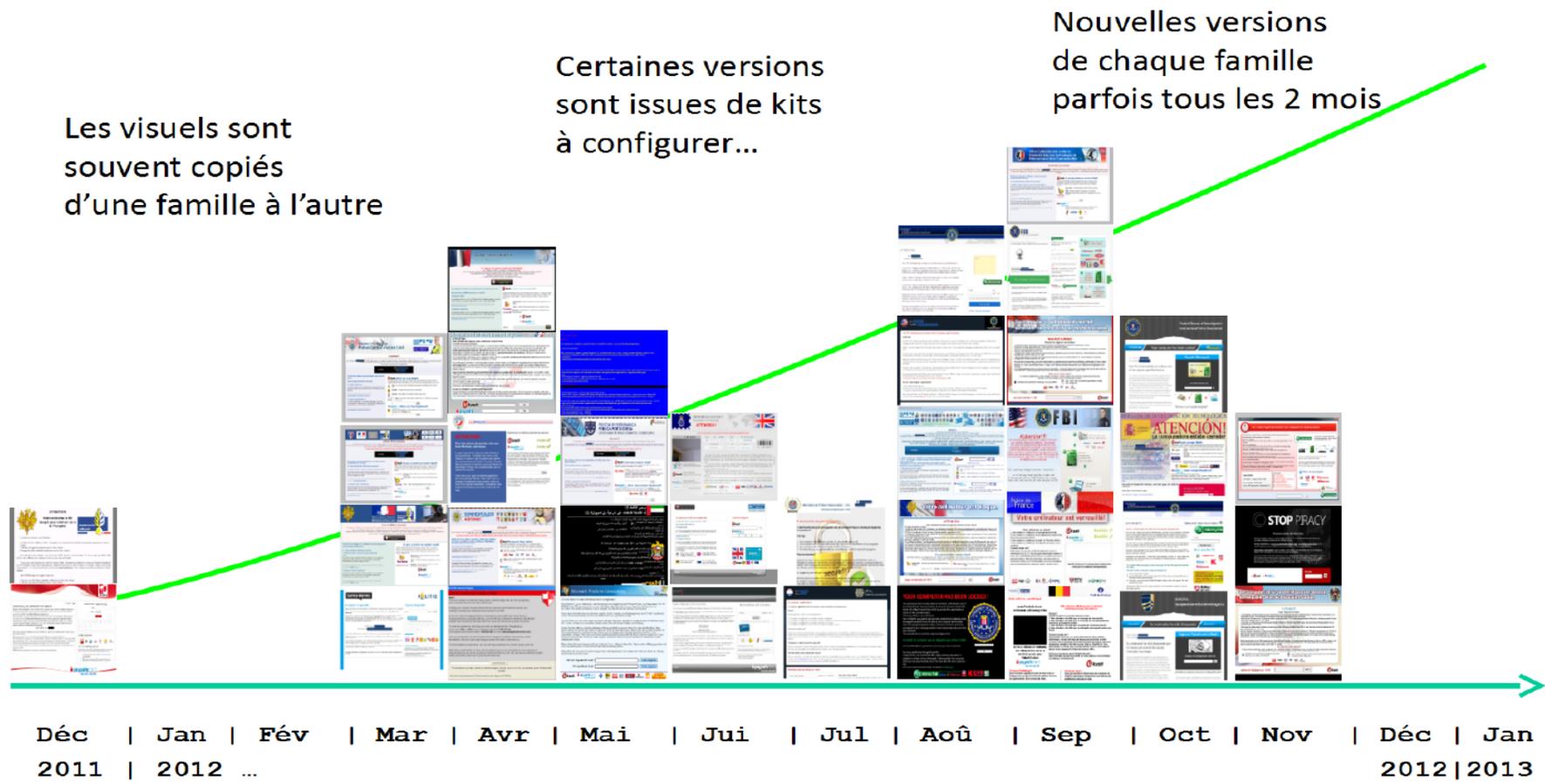
Vous pouvez payer l'amende avec l'aide des vouchers Ukash de 200 €. Ensuite, ouvrez le tab «Payer amende», remplir le fo «Payer amende». Votre ordinateur sera débloquent dans les 24 heu

Après le débloquent, nous suggérons que vous:

- Supprime toutes les fichiers multimédia en infraction avec le
- Supprime des logiciels en infraction avec les droits d'auteur
- Installer un logiciel anti-virus, si vous n'en avez pas encore.

- 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

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



Source: E. Freyssinet, Lutte contre les botnets

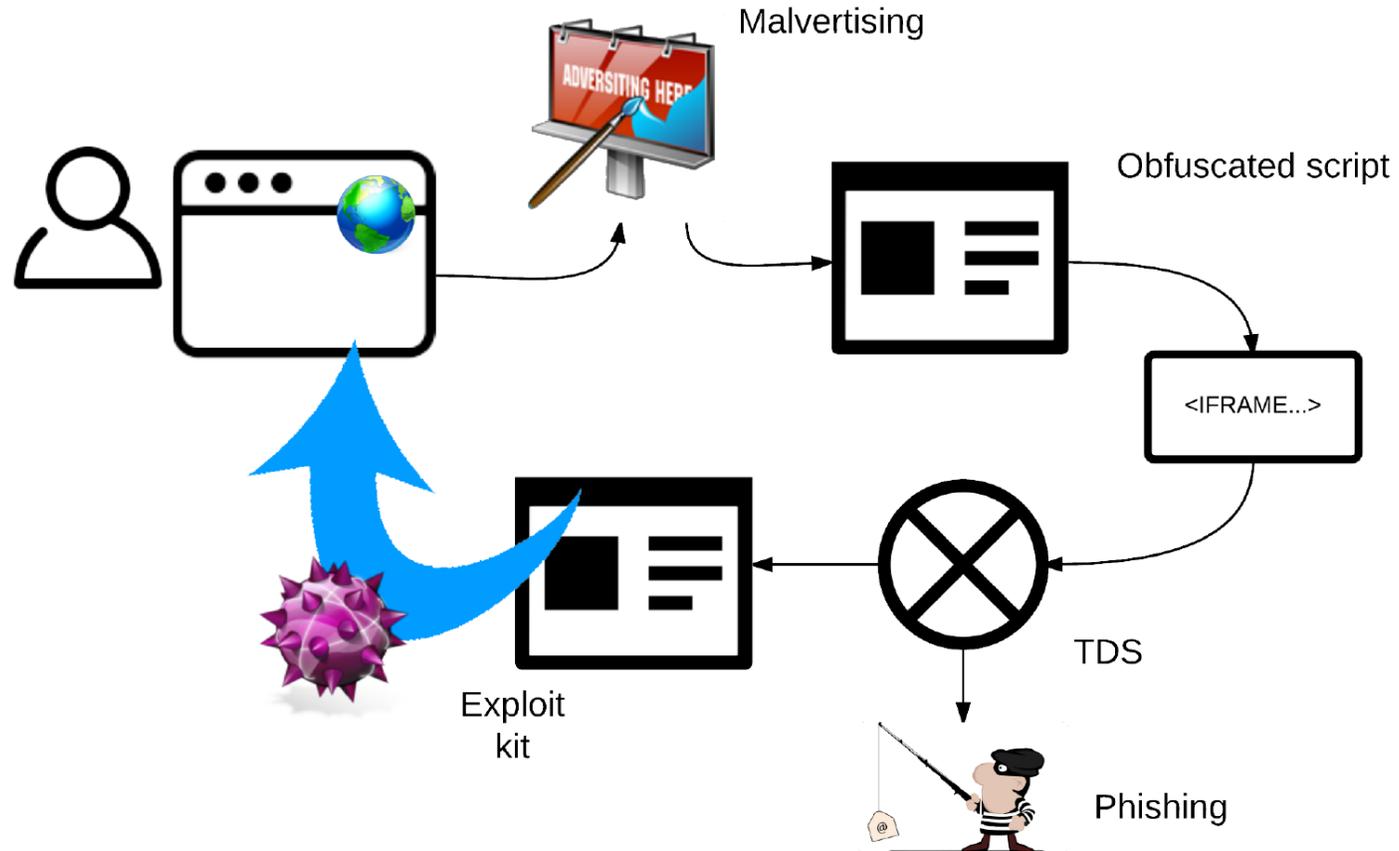
TLP:WHITE

CRYPTOLOCKER – L'AVÈNEMENT DES RANÇONGIERS CHIFFRANTS

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

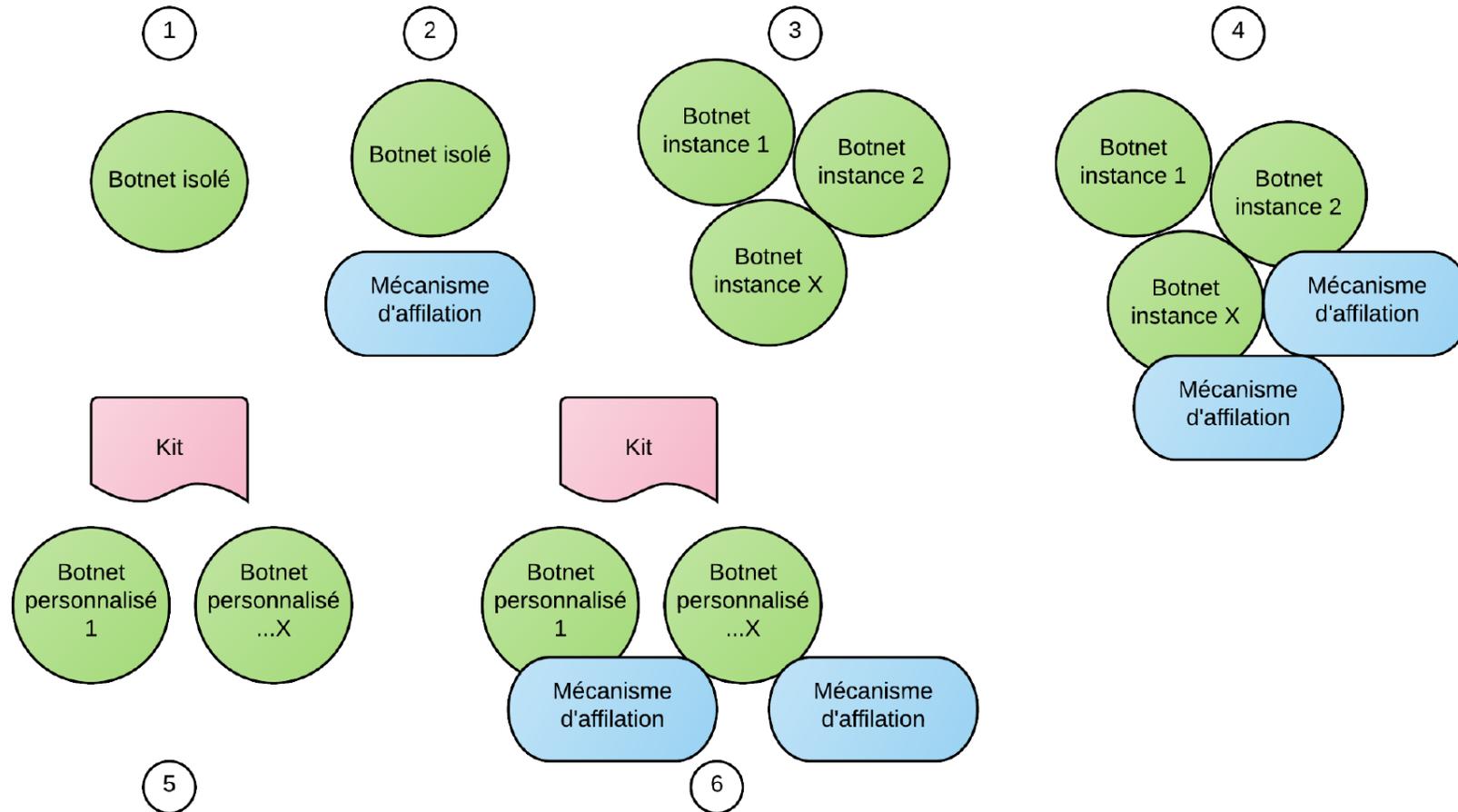


SCHÉMA TYPE DE DISTRIBUTION DES LOCKERS PAR « MALVERTISING »



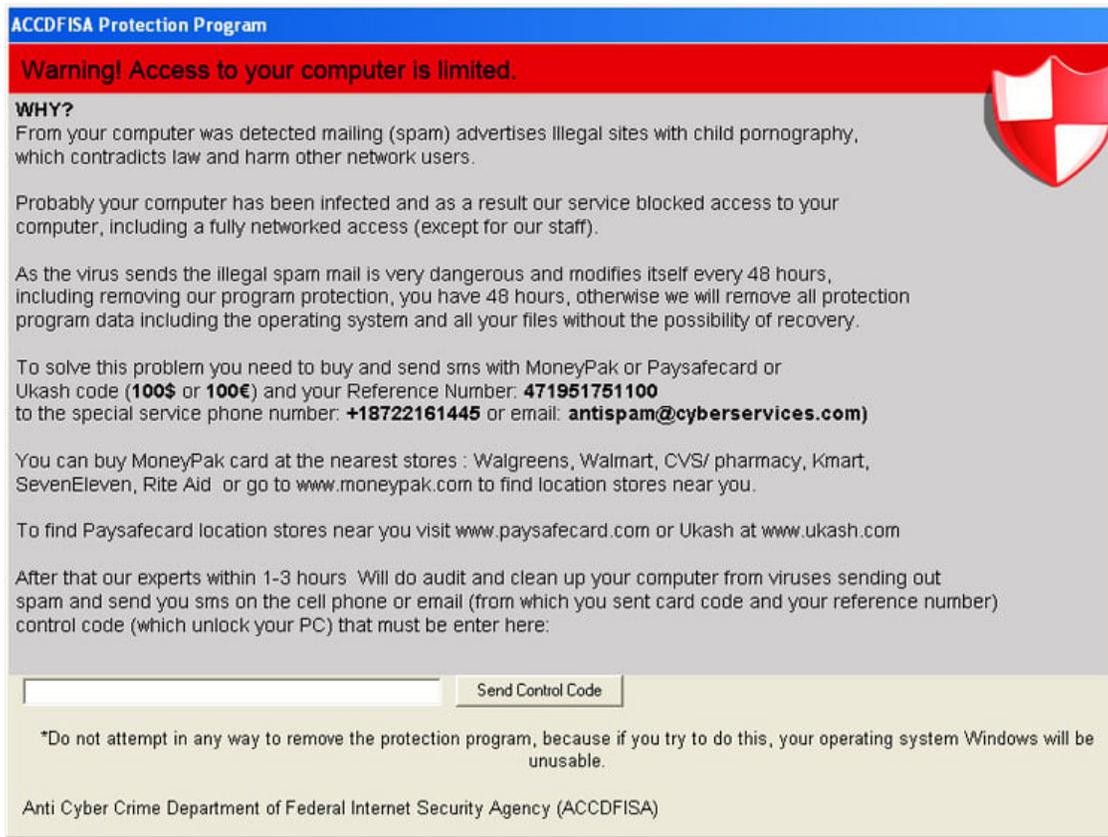
Source: E. Freyssinet, Lutte contre les botnets

DIFFÉRENTES ARCHITECTURES POSSIBLES



Source: E. Freyssinet, Lutte contre les botnets

ACCDFISA – CIBLAGE DES RÉSEAUX D'ENTREPRISE



ACCDFISA Protection Program

Warning! Access to your computer is limited.

WHY?
From your computer was detected mailing (spam) advertises illegal sites with child pornography, which contradicts law and harm other network users.

Probably your computer has been infected and as a result our service blocked access to your computer, including a fully networked access (except for our staff).

As the virus sends the illegal spam mail is very dangerous and modifies itself every 48 hours, including removing our program protection, you have 48 hours, otherwise we will remove all protection program data including the operating system and all your files without the possibility of recovery.

To solve this problem you need to buy and send sms with MoneyPak or Paysafecard or Ukash code (**100\$** or **100€**) and your Reference Number: **471951751100** to the special service phone number: **+18722161445** or email: **antispam@cyberservices.com**)

You can buy MoneyPak card at the nearest stores : Walgreens, Walmart, CVS/ pharmacy, Kmart, SevenEleven, Rite Aid or go to www.moneypak.com to find location stores near you.

To find Paysafecard location stores near you visit www.paysafecard.com or Ukash at www.ukash.com

After that our experts within 1-3 hours Will do audit and clean up your computer from viruses sending out spam and send you sms on the cell phone or email (from which you sent card code and your reference number) control code (which unlock your PC) that must be enter here:

*Do not attempt in any way to remove the protection program, because if you try to do this, your operating system Windows will be unusable.

Anti Cyber Crime Department of Federal Internet Security Agency (ACCDFISA)

- 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)

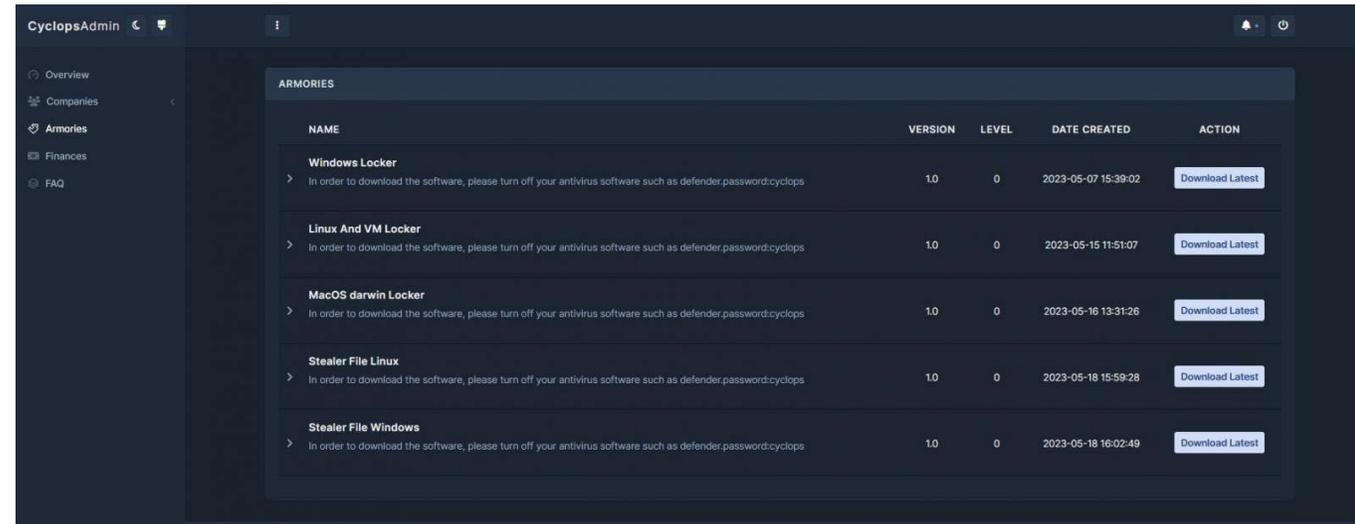
<https://www.emsisoft.com/en/blog/818/the-accdfisa-malware-family-ransomware-targetting-windows-servers/> TLP:WHITE

PREMIER BILAN

- Les rançongiciels (chiffnants) 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

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



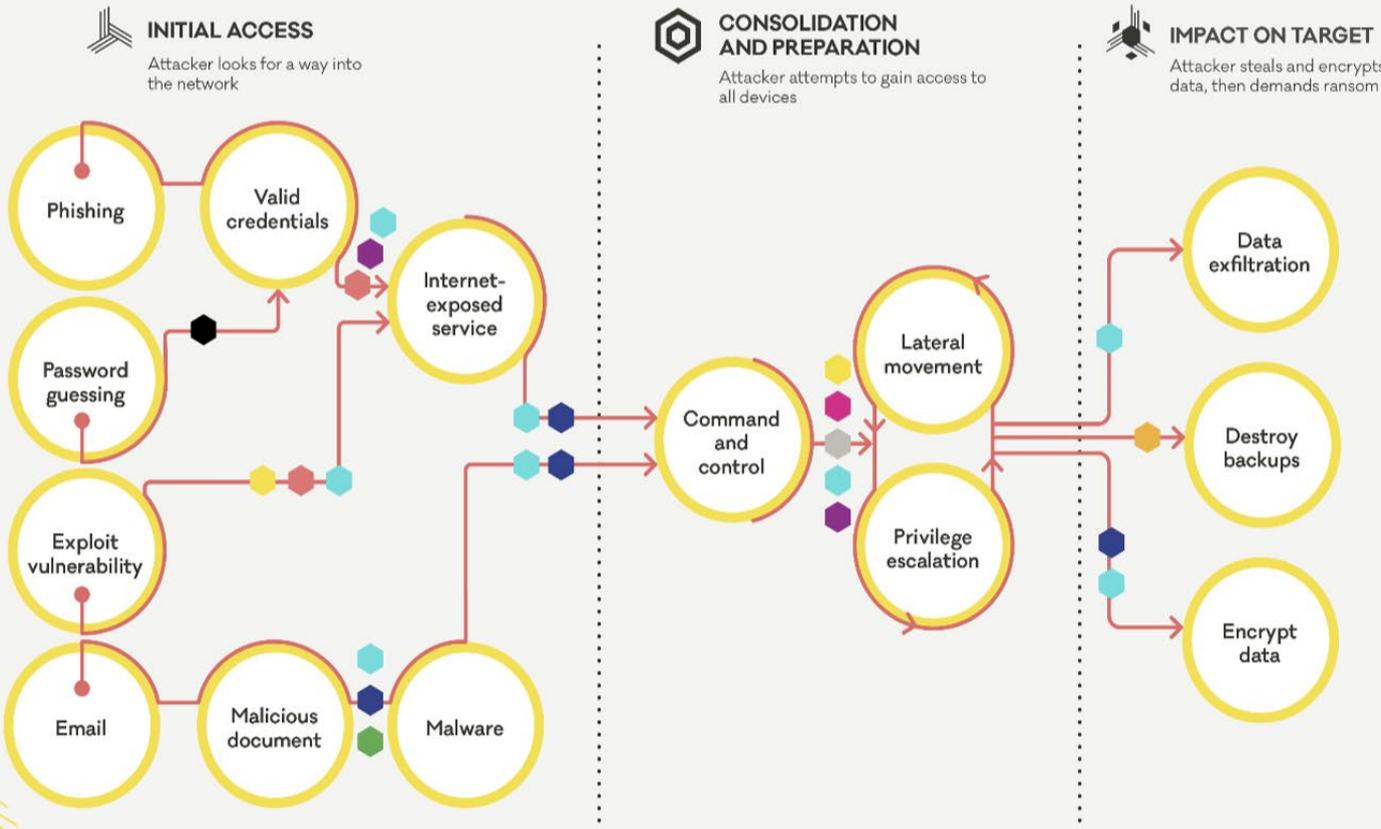
Ex. panel Cyclops de distribution de logiciels malveillants ciblant différentes plateformes (source Bleepingcomputer)

CYCLE TYPIQUE DES RANÇONGIERS AUJOURD'HUI

LIFECYCLE OF A RANSOMWARE INCIDENT

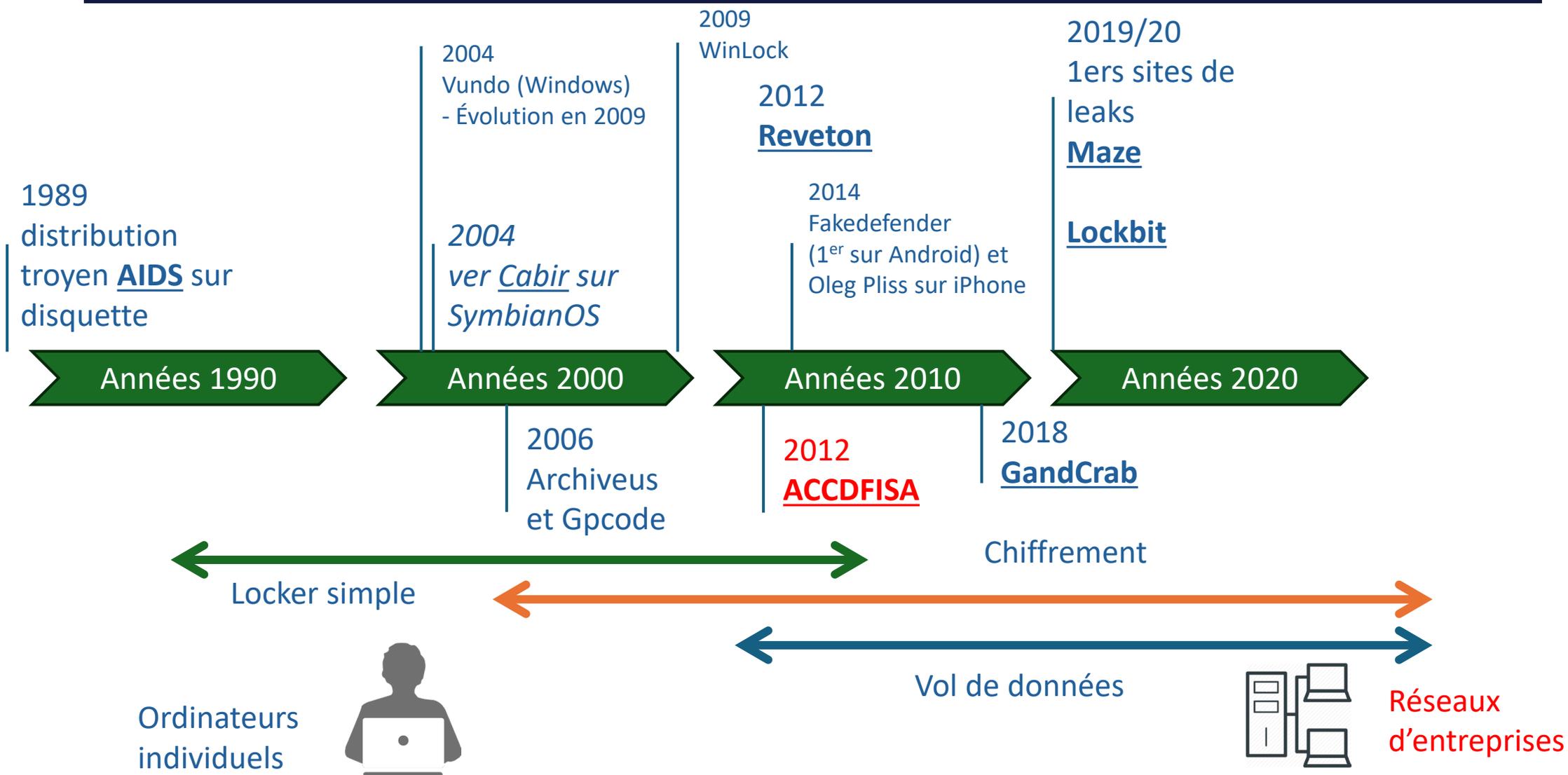
How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.

certnz



- 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)

HISTORIQUE DES RANÇONGIERS



QUE RETENIR

- **En résumé, le rançonnement 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 ? PME et particuliers.
- Rançonnement 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...)

QUESTIONS



TLP:WHITE