# Attention, on vous surveille…

30 septembre 2021

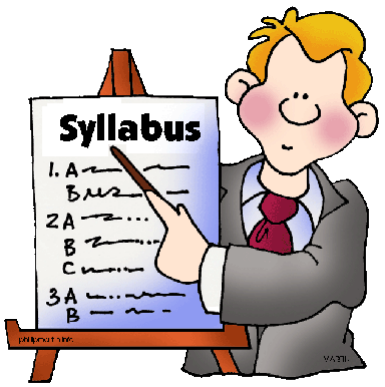



claude@lemarson.com
https://www.lemarson.com

## Sommaire

**Attention, on vous surveille**






Le RAT, c'est comme le GPS espion dans une voiture. Il nous suit à la trace…

# Notre vie privée en danger

## Des attaques d'un nouveau genre


Ingénierie sociale

"Remote Access Trojan"


Deep fakes

Ransomware



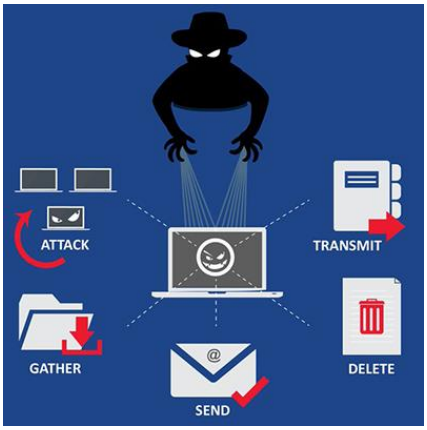
IA

- Les technologies convergent vers toujours moins de sécurité, de confidentialité et de protection de la vie privée
  - Ransomware
  - Ingénierie sociale
  - RAT (Remote Access Trojan)
  - Deep fakes associées à des vidéos : impossible de détecter les supercheries
  - IoT et l'absence de protection des objets usuels
  - Cryptographie
  - IA
  - Faiblesse sécuritaire des infrastructures Internet et mobiles : décalage entre les protections et les risques
- Qui nous observe :
  - Les GAFAM
  - L'administration fiscale
  - Les vendeurs de produits
  - Les criminels en tous genres, les mafias
  - Les services de renseignement de pays étrangers (Pegasus)
  - Les déstabilisateurs d'entreprises qui diffusent des documents "authentiques" vidéos ou autres.
- Immense naïveté et pratiques dangereuses : "cela n'arrive qu'aux autres…"



# Deux natures d'attaques

- Tous les moyens sont bons pour pénétrer les machines cibles
- Une fois dans la place, spyware ou ransomware, hors protections avancées, la partie est perdue…
- Un RAT ("Remote Access Trojan") est un outil de prise de contrôle à distance, très proche d'un outil légal, mais destiné à effectuer des opérations criminelles.
- Donne un accès complet aux machines, PC, tablettes et de plus en plus smartphones (la cible privilégiée est Android de Google).
- Un RAT peut être attaché à un fichier légitime, un document, un jeu vidéo, un courriel ou être téléchargés depuis un site Web "normal".
- La plupart des navigateur actuels réagissent bien et sont correctement protégés.
- Deux natures d'attaques RAT :
  - Ciblées : une personne fragile ou potentiellement intéressante… financièrement
  - Globales de plusieurs millions de machines : les hackers jouent sur le nombre, plus que sur la qualité
- Ce qui nous protège :
  - Les criminels ne doivent pas se faire prendre…
  - Il faut que le jeu en vaille la chandelle
  - Une attaque ciblée RAT nécessite de la compétence, de passer du temps sur la compréhension et l'intérêt de la cible
  - Ils doivent s'appuyer sur une plate-forme d'administration complète : le but n'est pas seulement d'envoyer des RAT
  - La phase post RAT est plus lourde et compliquée que l'attaque proprement dite



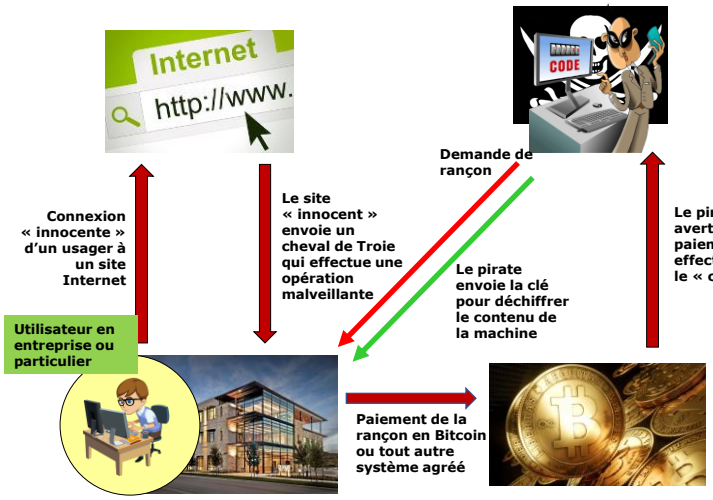
# RAT, comment en sommes nous arrivés là

- Il y a eu plusieurs générations de RAT
- On passe de la plaisanterie (de mauvais goût) dans les années 90 à l'industrie du "ransomware"
- Les premiers RAT étaient des amusements d'adolescents
- NokNok, D.I.R.T, NetBus, Back Orifice (référence à Back Office de Microsoft), SubSeven
- Ca se gâte en 1999 avec l'affaire Magnus Eriksson, professeur à l'Université Lund en Suède
  - Il "récupère" à son insu NetBus (écrit en 1998 par Carl-Fredrick Neikter)… et 12 000 fichiers pornographiques, dont 3 500 à connotation pédophile
  - Les administrateurs s'en aperçoivent, Eriksson est condamné et il perd son emploi.
  - Eriksson est réhabilité en 2004… mais le mal était fait.
- SubSeven date de la même période. Un vrai RAT.
  - Il redémarre Windows, inverse les boutons de la souris, enregistre des sons à partir du micro et des séquences vidéos à partir de la webcam, change les couleurs du bureau, ouvre et ferme le lecteur de CD-ROM, prend des copies d'écran, allume et éteint l'écran !
- A partir des années 2000, fin de l'angélisme. L'objectif c'est de gagner de l'argent et tous les moyens sont bons.
- Le nombre de RAT explose et des malwares de prise de contrôle malveillants font beaucoup de dégâts : NetWire, NanoCore, ImminentMonitor, Ozone RAT, OmniRAT, Luminosity Link, SpyNote, Android Voyager, Web Monitor
- En 2021, les dernières versions de RAT, Ransomware 2.0, deviennent des vecteurs imparables de pénétration furtive.
- Il y a actuellement près de 1 000 RAT, certains gratuits, d'autres en vente libre dans le dark web

Le setup de SubSeven
(Netbus à l'envers avec Seven qui remplace ten)



# Le « ransomware »




- Les demandes de rançon sont fondées sur le chiffrement des contenus, par des algorithmes à clés secrètes.
- Les criminels créent leurs propres algorithmes, ce qui rend très difficile le décryptage "aveugle".
- Les algorithmes utilisés sont de plus en plus sophistiqués, ce qui est lié aux compétences mathématiques : Russie, Chine, pays de l'ex Europe de l'est.
- Le "ransomware" devrait représenter 20 G$ de pertes globales en 2021, avec la perte de production.
- 1/3 des victimes payent une rançon.
- Stratégie : être paranoïaque, faire des sauvegardes systématiques et… ne pas payer les rançons, sauf cas extrême
- Tendance : les criminels envoient de moins en moins la clé qui a servi à l'attaque.
- Ne jamais laisser accessibles les supports de sauvegarde : NAS…
- 50 % des entreprises américaines ont eu à faire face à des attaques de ransomware en 2020
- La moyenne des rançons pour les grandes entreprises a été de 180 000 $ et de 6 000 $ pour les PME
- Une nouvelle attaque de ransomware est déclenchée toutes les 11 sec.

# L'ingénierie sociale


**Phishing**
ou l'art de convaincre l'interlocuteur de fournir des informations confidentielles


**Vishing**
convaincre un interlocuteur au téléphone, d'effectuer une opération malencontreuse


**Clickjacking**
inciter les inbterlocuteurs à visiter tout autre chose que ce pour quoi ils sont venus

**Dumpster diving**
récupération des informations envoyées dans les corbeilles


**Nigerian Scam**
Faire croire aux victimes qu'elles ont été choisies... Plus la ficelle est grosse, plus ça passe...

**Baiting**
laisser un suport amovible sur les lieux de la victime, qui contient un logiciel malveillant


**Friendling**
Donner confiance en jouant sur des amis communs, que l'on peuyt trouver dans les résdeaux sociaux


**Pretexting**
Capacité à se construire une identité qui donne confiance aux interlocuteurs

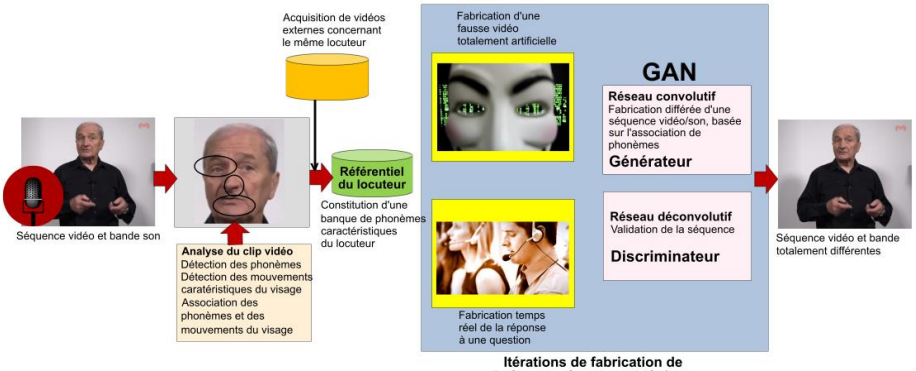

**Typosquatting**
incitation à cliquer sur des liens URL dont le nom est proche de celui des sites les plus connus


**Réseaux sociaux**
récupération de nombreuses données "intéressantes" disponibles dans les réseaux sociaux

- L'ingénierie sociale concerne deux natures d'attaques : celles qui visent le système d'information et se fondent sur des techniques éprouvées de récupération d'informations confidentielles auprès des personnels de l'entreprise et celles qui s'intéressent à la pénétration physique des locaux
- Attaques non physiques, l'ingénierie sociale « fonctionne » selon une séquence quasi-immuable :
  - Recueil d'informations sur la cible
  - Etablissement d'un rapport de confiance entre la victime et son assaillant
  - Exploitation des failles et techniques d'infiltration
  - Exécution de l'attaque
- Ces attaques nécessitent de la part des attaquants des « qualités » spécifiques :
  - L'art de poser les bonnes questions au bon moment : l' « élicitation »
  - La capacité à jouer un rôle et à se faire passer pour quelqu'un d'autre
  - L'art de la tromperie
  - L'art de la persuasion.



# Deepfake




**Itérations de fabrication de la fausse séquence vidéo/son**

- « deep fake » : concaténation de « deep learning » et de « fakes » (faux). Plus probablement le pseudo repris d'un utilisateur de Reddit, qui avait exploité le « deep learning » pour intégrer les visages de célébrités dans des films pornographiques.
- C'est l'art de nous faire croire que la personne qui s'exprime sur une vidéo est bien réelle et qu'elle prononce (ou a pronorcé) les phrases que nous entendons. La supercherie se répand très vite.
- Quelques "réalisations" : qui ont fait le tour du monde
  - Mark Zuckerberg, qui se vante de contrôler ses utilisateurs (c'est faux ?)
  - La présidente de la Chambre des Représentants à Washington, Nancy Pelosi, qui apparaît dans un état d'ébriété avancé.
  - Dans le même créneau, le visage du président argentin Mauricio Macri a été remplacé par celui d'Adolf Hitler et celui d'Angela Merkel, par Donald Trump.
- La question est de savoir si la technologie va s'étendre au temps réel et envahir les fausses plates-formes de service.

# Les fonctions d'un RAT

- L'objectif des RAT, des malwares qui se modernisent, est d'obtenir les mêmes droits que les victimes et d'agir en toute transparence.
- Récupération de documents et informations confidentielles : mots de passe, accès aux banques à distance, photos personnelles et intimes, fichiers audios et vidéos, tous exfiltrés vers des serveurs d'accueil : Russie, Chine, ex pays de l'Est de l'Europe, mais aussi aux USA, Canada, France…
- Activation sans autorisation de la webcam et du micro, parfois discrètement, lancement des enregistrements et récupération des fichiers vidéo.
- Accès administrateur aux machines, pour installer des malwares et effectuer toutes les opérations habituelles de "service" : formatage du disque dur
- Lancement d'opérations illégales et embarrassantes au nom des victimes
- Récupération de contenus illégaux, avec paiement effectué par les victimes
- Configuration des machines en proxy pour commettre des actions illégales de manière anonyme
- Constituer des infrastructures de botnets
- Lancement d'attaques DDOS
- Minage de bitcoins
- Hébergement de fichiers illégaux
- Keylogging pour récupérer des données confidentielles
- Demandes de rançon en jouant sur l'aspect intime et très personnel des informations capturées

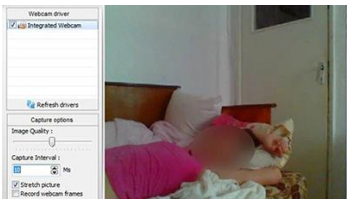

Ne pas confondre avec : « Cher Monsieur **Dujambon**, nous avons une vidéo de vous en train de tromper votre femme la nuit de **5 octobre** au **Marriott de Montréal**. Nous allons envoyer cette vidéo à votre femme au **18 route des hackers repentis à Genève**, si vous ne payez pas 1 000 $ CAD dans la journée. N'essayez pas d'appeler la police, car votre téléphone **1 514 123 45 67** est sous écoute ».



# Haha, you got RATted!

- Dès lors que l'on se sert d'une machine, il faut considérer que l'on est dans un espace public et donc susceptible d'être pollué par des perturbateurs et hackers.
- On n'est plus dans son salon…
- La diffusion de vidéos volées est un viol et doit être puni comme tel.

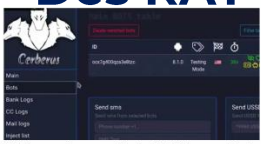





**Suggestion pour se protéger**

- Exploitation d'une cyber technologie issue des labs ultra-secrets américains, un mélange très sophistiqué d'IA, de cryptographie elliptique et de réseaux neuronaux convolutifs : le sparadrap.
- Consiste à découper un morceau de sparadrap et à le coller sur l'œil de la caméra de la machine.
- Technologie libre de droit, tombée dans le domaine public, que l'on doit à Oscar Troplowitz (un pharmacien allemand).
- Il faut simplement penser à le retirer quand on a besoin de la caméra.
- On peut aussi utiliser des stickers, des cache caméras…

# Des RAT « effrayants »… à ne pas utiliser




RAT bancaire pour Android. Très sophistiqué. A largement été diffusé, le source est disponible chez les hackers.
Dangereux, capable de voler les codes 2FA (y compris ceux de Google), vise les banques à distance. Très rapide.
Nombreuses fonctions de RAT.


Outil RAT complet d'administration de nos machines. L'un des plus dangereux.
Récupère les mots de passe, peut être configuré comme proxy HTTP, capture audio et vidéo Webcam, keylogger.
Peut encore servir de tracker IP…

NjRat Danger Edition. Version orientée d'un précédent NjRat. Orienté finances.
Très récent et l'un des RAT les plus puissants.
Minage sur la machine victime. Modification de la base de registres, lancement d'attaques DDOS, démarrage et arrêt de la machine à distance. Vol de monnaies cryptographiques.
Déconnecte le gestionnaire de tâches.
Capable de s'arrêter quand il constate un processus de détection. Peut facilement être désactivé, car il consomme beaucoup de ressources (20 % du PC en moyenne).


Darkcomet (en principe arrêté). Assez ancien.
Développé par Jean-Pierre Lesueur, un français.
A été très utilisé pour surveiller des "activistes" pendant la guerre en Syrie.
Comporte une large panoplie de fonctions RAT : keylogging, vol de mots de passe, contrôle des machines.
A été téléchargé (entre autres) par un lien #JeSuisCharlie", à la suite de l'attentat contre Charlie Hebdo (en fait, le lien menait à un téléchargement de Darkcomet). La technique utilisé était la stéganographie (image d'un enfant) associée au téléchargement furtif ("drive by download".


Orcus RAT. Présenté souvent comme un clone de TeamViewer. Ne coûte que 40 $… avec toutes les fonctions illégales. Récupère les mots de passe, keylogger.
Très orienté vers le son et vidéo. Peut activer le micro et enregistrer des séquences. Peut activer la vidéo, dont il cache le voyant d'activité, pour enregistrer des séquences personnelles.


RAT pour Android. Orientation bancaire. Vole les identifiants des portefeuilles de cryptomonnaies et des cartes bancaires. Récupère toutes les données système et prend le contrôle des machines.
Capture d'écrans, enregistrement de séquences sonores et vidéos, keylogging, peut être configuré pour faire transiter le proxy de réseau.


Exfiltre les fichiers, vole les portefeuilles de cryptomonnaies, keylogging, active et enregistre les vidéos Webcam, etc.
En vente dans de nombreux forums, entre 100 et 600 $, mais a été cracké…
Attaque uniquement les machines Windows.



# Exemples rendus publics

- Les statistiques sont rares… car les victimes ne se plaignent pas, par honte ou peur et ne lancent pas (sauf exceptions) de procédures judiciaires.
- Tout dépend de la nature des "objets" volés.
- Conséquences :
  - Pertes financières.
  - Exfiltration de données sensibles d'entreprises. Des DSI ont été attaqués et ont mis en péril leur système d'information.
  - Dépressions inexpliquées, car inexplicables.
  - Tentatives de suicides.
  - Repli sur soi, chez les plus jeunes…
- La sextorsion, bientôt sport olympique…
  - Ne pas confondre avec le chantage exercé avec la complicité de la victime, qui a fourni elle-même les éléments pour se faire attaquer
- L'affaire Cassidy Wolf, miss Teen USA avec James Abraham (20 ans), Gary Kazaryan (105 ans requis contre lui),
- Un britannique de St Helens en Angleterre est condamné en 2020 à 2 ans de prison pour usage du RAT Imminent Monitor (IM-RAT) a des fins de chantage sexuel par prise de contrôle de caméras.
  - Confondu car il avait utilisé son vrai nom et courriel pour acheter via Paypal le RAT IM-RAT
- Philip Durachinsky (Ohio) espionne des milliers de machines pendant 14 ans avec FruitFly : écoles, entreprises, structures gouvernementales, Police…
  - Prise de contrôle des caméras
  - Se fait prendre quand il s'attaque à sa propre Université


James Abrahams Cassidy Wolf

Philip Durachinsky

# L'affaire (inquiétante) Pegasus

- Très significative affaire du spyware Pégase
- Spyware créé par la compagnie israélienne NSO Group (spécialiste de sécurité), pour surveiller les terroristes : 60 grands clients dans 40 pays
- Que faut-il en penser ?
- …surveille aussi des victimes "innocentes" : journalistes, organisations axées sur les droits de l'homme, diplomates et grands patrons
- Techniquement, le processus est simple : NSO Group envoie un lien sur un mobile iOS 14.6, qui une fois activé installe le malware, sans interaction avec le propriétaire du smartphone
- Pegasus accède aux messages, carnets d'adresses, historiques des appels, localisations géographiques, calendriers, historiques de navigation sur Internet…
- Pegasus "fait plus de choses" que le propriétaire du smartphone
- Il peut activer le micro, la caméra, lancer des appels, effectuer des enregistrements qu'il envoie en toute transparence à une adresse
- Le scandale éclate par Amnesty International et divers médias du monde entier
- Le gouvernement marocain est pris la "main dans le sac", pour sa surveillance du président français Emmanuel Macron, ainsi que divers journalistes et avocats français…
- La liste noire des personnes surveillées comporte 50 000 noms…
- Il n'y a pas d'espace entre les activités légitimes de NSO Group et de ses clients et celles qui ne le sont pas…
- Il ne faut pas être hypocrite : qui est responsable ?


**Pégase,** cheval ailé de la mythologie grecque sert de monture à Bellérophon pour vaincre la **Chimère…**
**Inutile de le savoir, mais ça peut servir dans les dîners en ville…**



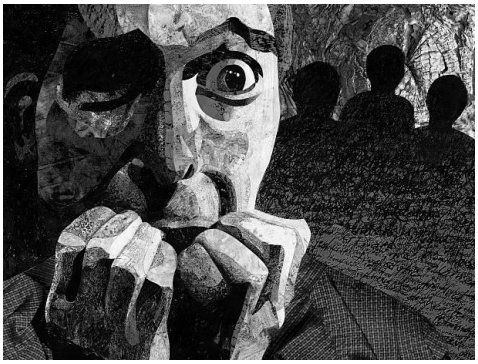
# Le cas de l'iPhone

- Beaucoup plus imperméable aux RAT que les mobiles Android.
- Pour pouvoir prendre le contrôle de l'iPhone et de sa caméra, il faut installer un logiciel, issu d'un autre espace que l'Apple Store.
- Impossible sauf si l'iPhone a été "jailbreaké" (débridage), qui consiste à outrepasser les protections natives d'iOS.
- Demande une grande compétence technique, hors de portée de la majorité des hackers individuels, mais pas des organisations étatiques ou mafieuses.
    - Controverse de l'attentat de San Bernardino
- Pas d'attaque de type RAT recensée à la fin 2021

# Les précautions à prendre

## Ne pas se demander si cela va arriver, mais... quand cela va arriver

- Compte tenu des faiblesses natives des protocoles Internet, il est illusoire de se prémunir contre les RAT et logiciels de prise de contrôle : cela reviendra toujours à cautériser une jambe de bois.
- Si l'activité est sensible, il faut être paranoïaque.
- On peut "ad minimum" ne pas tenter le diable
  - Vérifier que notre  pare-feu est activé : près de 80 % des utilisateurs(hors entreprises) n'en voient pas l'utilité, si ce n'est de les empêcher de travailler
  - Vérifier que les logiciels présents dans les machines cibles sont mis à jour : les éditeurs n'ont pas pour vocation de créer des portes dérobées…
  - Interdire (comment ?) le téléchargement de documents issus de sources non sûres… Sauf à brider totalement la machine…
  - Ne pas cliquer sur des liens douteux, ni participer à des boîtes de dialogue suspectes
  - Procéder à des sauvegardes automatiques et systématiques sur la base d'un plan de sauvegarde précis
  - Disposer d'un anti malware à jour, dédié chevaux de Troie et spywares (les technologies sont proches des RAT) : la technique de détection des RAT est en général assez simple, avec des indices clairs
  - Prévoir un plan de secours personnel lorsque l'écran redouté apparaîtra et le tester régulièrement.
  - Anticiper sur les recours techniques et juridiques.

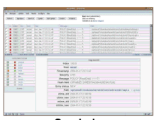


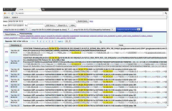


# Les meilleures protections

- Il n'y a pas de détecteurs dédiés RAT… qui ne fassent que cela.
- Le choix est à faire parmi des solutions dont la chasse au RAT et à la prise de contrôle "sauvage", est une fonction parmi d'autres.
- Il existe de nombreux comparatifs, celui de Stephen Cooper de Comparitech est un bon exemple

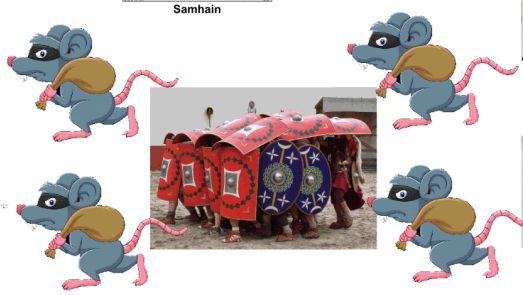

Solarwinds Security Event Manager

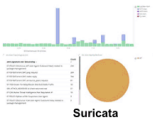

Samhain


Zeek


Sagan

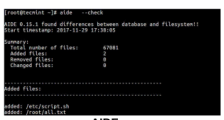

OSSEC

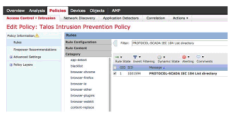


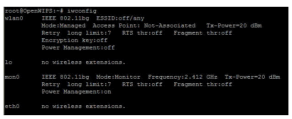

Suricata


831


Security Oignon


AIDE


Snort

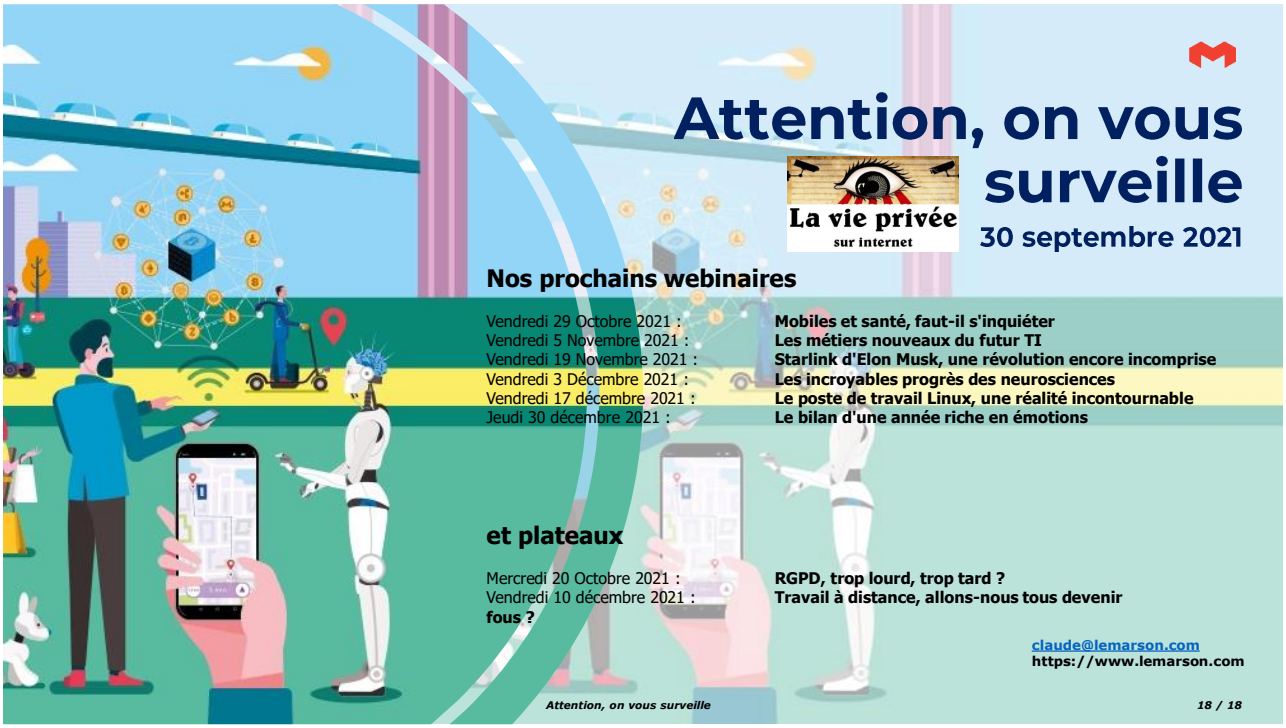

OpenWIPS-NG

# Ce à quoi, il faut s'attendre

- Les attaques personnelles seront de plus en plus ciblées et nombreuses : même logique que les enlèvements.
- Forme aboutie de lâcheté anonyme.
- Il est devenu quasiment impossible de se protéger et les contraintes règlementaires type RGPD n'ont plus de sens dans ce contexte. Elles ont 1000 ans de retard.
- Les cibles les plus risquées sont les enfants, du fait de leur usage irraisonné des mobiles.
- Les machines ne sont pas suffisamment protégées et les protocoles d'accès aux "devices" sont à la portée de n'importe quel RAT : une nouvelle architecture des contenus est à imaginer, sur le même principe que celui de "runtime" hyperprotégés (pas une garantie absolue) où s'exécute le noyau de l'OS.
- Les techniques d'IA et de deep fakes vont considérablement modifier la nature et le fonctionnement des RAT.
- Il faut se préparer à un état de guerre permanent, la protection de la vie privée devenant impossible à assurer dans la vie courante…
- Des formes de "viols" numériques sont à envisager, qui auront les mêmes conséquences sur les personnes fragiles : suicides…
- Une médecine spécialisée est à mettre sur pied, qui concernera tout le monde.
- Les cadres juridiques ne seront pas harmonisés, les états (voir RGPD) n'arrivant même pas à s'entendre sur l'âge d'un enfant.
- On peut considérer cette forme d'attaque très sophistiquée, comme le ransomware 2.0.
- Suprême inquiétude : avec les deep fakes, il n'est plus nécessaire de pénétrer les machines et voler des images compromettantes : il suffit d'une photo ou vidéo normale trafiquée en deep fakes pour obtenir les mêmes résultats


## La vigilance est indispensable, mais elle ne suffira pas





# Attention, on vous surveille

La vie privée sur internet

30 septembre 2021

## Nos prochains webinaires

| | |
|---|---|
| Vendredi 29 Octobre 2021 : | **Mobiles et santé, faut-il s'inquiéter** |
| Vendredi 5 Novembre 2021 : | **Les métiers nouveaux du futur TI** |
| Vendredi 19 Novembre 2021 : | **Starlink d'Elon Musk, une révolution encore incomprise** |
| Vendredi 3 Décembre 2021 : | **Les incroyables progrès des neurosciences** |
| Vendredi 17 décembre 2021 : | **Le poste de travail Linux, une réalité incontournable** |
| Jeudi 30 décembre 2021 : | **Le bilan d'une année riche en émotions** |

## et plateaux

| | |
|---|---|
| Mercredi 20 Octobre 2021 : | **RGPD, trop lourd, trop tard ?** |
| Vendredi 10 décembre 2021 : | **Travail à distance, allons-nous tous devenir fous ?** |

claude@lemarson.com
https://www.lemarson.com