Autodéfense Numérique

Notes du stream Au Poste ! de DavDuf du 15 novembre 2021 avec la Quadrature du Net, représentée par Nono, responsable technique et sysadmin, et axel simon (@axelsimon), membre et « expert en sécurité informatique » (ouhhh).

Principes généraux

1. Réfléchir en spectre de protection, pas en noir et blanc (protégé/pas protégé) : on est dans la gestion du risque, pas un concours de pureté ou un film d'espionnage
2. Réfléchir à son «?modèle de menace?», qui sera différent selon les personnes, les contextes, les moments dans le temps…
3. Penser à cloisonner, comme on le fait dans sa vie de tous les jours en étant différentes personnes selon les contextes (parent, ami, employé, etc.). Ce qui veut dire faire différentes choses sur différentes machines, différents logiciels, comme par ex ne faire certaines recherches que par le navigateur Tor (Tor Browser)
4. Différents adversaires ont différents moyens : tout le jeu est de mettre assez de protections en place pour rendre les attaques trop, difficiles, trop longues ou trop coûteuses (ou une combinaison des trois)
5. Respirer : à moins d'avoir un modèle de menace vraiment vénère, c'est ok de se planter de temps en temps ou de baisser son niveau de protection à des moments pour faire certaines choses.

Ressources

- Brave ?
    - Plutôt Firefox, Brave remplace les pubs des régies publicitaires par les siennes, déplaçant le problème
- Firefox
    - extensions qu'on aime bien :
        - uBlock: plusieurs filtres

        - privacy badger
        - Cookie Autodelete
        - Decentraleyes
        - Location Guard
- Services mails poubelle:
    - mailinator.com
    - guerillamail.com
    - https://www.shitmail.org/
    - https://10minutemail.com/?lang=fr
- Applications ou systèmes utiles :
    - https://www.torproject.org/ : réseau pour anonymiser son trafic internet
    - https://tails.boum.org/ : version de Linux qui permet de démarrer un ordinateur sur un système temporaire, amnésique et incognito (ie: anonyme, car faisant passer tout le trafic par Tor). TAILS: the Amnesic Incognito Live System
    - https://www.whonix.org/ : Distiribution Linux spécialisé dans la securité et l'anonymat qui utilise des VM pour une meilleur isolation.
    - https://www.qubes-os.org/ : QubesOS est un système d'exploitation orienté sécurité par compartimentation. Pas évident à utiliser au quotidien et demande une machine assez puissante, mais c'est un chouette projet.
- Hebergeur mail militant
    - Riseup : https://riseup.net/
    - Autistici/Inventati : https://www.autistici.org/
- Anonymisation du trafic Internet
    - Tor : https://www.torproject.org/
        - https://nos-oignons.net/Diffusez/affichettes-tor-et-https.pdf
- Sources
    - https://jenairienacacher.fr/
    - https://guide.boum.org/

Le forum Technopolice, la campagne contre la surveillance de nos villes, par LQDN : https://forum.technopolice.fr

QUESTIONS :

Première question : la carte d'identité biométrique est-elle concernée ?
(Oui même si elle ne contient pas d'électronique)
https://www.laquadrature.net/2021/10/07/carte-didentite-biometrique-sa-genese-macronienne/

Enjeux numériques aujourd'hui : les données récoltées ; les façons dont elles sont utilisées

A-t-on perdu la bataille de l'autodéfense : C'est compliqué, on ne l'a pas perdue, mais il n'y a pas de dichotomie protégé-e - pas protégé-e. Le risque 0 n'existe pas !

- Jusqu'à quel point l'autodéfense numérique est-elle pertinente avec la mise en place progressive des boîtes noires? vu
- VPN ? vu
- Y a t il des outils qu'on utilise couramment en les pensant sur et qui sont vérolés ?

  - - Proton ? Signal ? Telegram ? Veracrypt ? (Briar+++ = pas besoin de serveur central)

- Y a t il une boite mail vraiment sure ? Ou du moins moins pire ?
- il faut vraiment abandonner Google chrome ? et Google en général (mail, moteur de recherche etc...) Tu peux très bien utiliser les outils de google d'une manière raisonnée et très attentive pour ne pas ou peu ("pas" c'est compliqué...) leur lâcher de données sur toi ! Il faut bien comprendre et être très attentif à ce que tu fais avec mais c'est possible
- est il envisageable que des groupes indépendants, des personnes faisant des logiciels libres, puissent reproduire des sites, applis existants pour en faire des logiciel libres (des sites de covoit, des reseaux sociaux etc etc). Ma relexion vient du fait que au départ bla bla car était gratuit puis est devenu payant je crois ? Je me suis souvent dit, ca doit pas être si compliqué de faire un site équivalent en accès libre ? mais peut etre que je me trompe complet !

  - - mobicoop par exemple :) Mais le soucis c'est le réseau autour de ce site ... On en parle dans 1 sec ;)

- on peut avoir le lien pour NoScript? : https://noscript.net (merci)
- Je repose ma question sur le tracage matériel? Mythe ou réalité? Que faire si il y a des backdoor dans mon pc par ex sur ma carte reseau? -> https://earsandeyes.noblogs.org/
- Si j'utilise un VPN, est-ce que mon adresse IP d'origine est réellement protégée? vu
- qq personnes du chat semblent sceptiques concernant la surveillance de l'état en disant qu'il manque de moyen et de compétences, qu'en pense les intervenants ? Moi je pense que si ils n'ont pas les moyens ils peuvent par contre demander aux privés qui les leur communiquerons ? Et je pense que cela intéresse l'état de savoir des choses sur nous. vu
- L'avis de davduf sur la démarche PeerTube de Blast (pour réduire la collecte de données par Twitch et Youtube)
- alors des fois tu vas sur un site tu as le rgpd qui impose une nouveauté sur la gestion des cookies certains jouent le jeu de ne pas obliger d'accepter et d'autres pas et donc compliqué non? https://www.laquadrature.net/2021/05/28/les-cookies-qui-sont-ils-que-veulent-ils/
- Existe-t-il des 'guides' simplifiés, accessibles à des personnes débutantes, pour se mettre en place un premier environnement sécurisé selon ses besoins ? (Le sujet étant large et l'ensemble des questions ne pouvant être répondues ce soir)
- c'est quoi leur avis sur freenet ?
- Question sur Tor : quel fut le moment où on a commencé à douter de la perfection de Tor ? Financement par le gouvernement US ? pas du tout, c'est financé par le gouvernement US depuis le début. Non il y a des bugs de sécurité plus ou moins mineurs de temps en temps et des attaques techniques possibles, dont une qui est connue depuis le tout début (un observateur qui est capable d'observer la trafic qui

sort d'une cible et sa destination probable: ie, mon ordinateur et le serveur auquel je me connecte), mais ces limites connues mises à part, in l'y a pas de faille majeure dans Tor, à ma connaissance. Comme toujours, il faut par contre absolument garder le logiciel à jour pour profiter de toutes les corrections de bugs (dont des bugs de sécurité).
- pour le meilleur respect de la vie privée, le mieux c'est un Pixel dégooglisé ?

- un système comme CalyxOS (ou GrapheneOS) c'est une grande, grande avancée déjà oui

- C'est quoi ce service où on peut avoir la fibre? https://fdn.fr est le fer de lance mais il y a beaucoup de FAI associatifs réunis au sein de la fédération https://www.ffdn.org/ et ils peuvent fournir d'autres services que l'accès à internet : VPN, hébergement, wifi de quartier, fibre, ADSL...
- qu'est-ce qu'il manque aux journalistes (au hasard David...) pour passer au logiciel libre ? Quels sont les points de blocages / frictions / manques qui rendent incontournables les GAFAM ? Si on peut contribuer au libre, sur quoi il faut mettre l'effort ?
- Si je peux commencer par une question piquante, parce qu'on me l'a posée y'a quelques jours : on connait l'effet "pied dans la porte", où un outil est utilisé d'abord pour le 'bien commun' (par exemple en santé), avant d'avoir d'autres utilisations. Par exemple, quels arguments donner contre les drones qui vont (à toulouse) transporter des médicaments à l'hôpital en urgence ?
- Est-ce que lQdN compte agir ou faire un recours contre la DSP2 (directive européenne sur les moyens de paiements) qui impose une authentification à deux facteurs pour accéder à son compte bancaire (le code de confirmation par SMS devenant insuffisant) et donc, impose aux citoyens européens d'être client Google ou Apple vu que cela impose d'avoir l'appli mobile pour accéder à son compte bancaire ? En tant que citoyen européen, on devrait pouvoir avoir un compte (droit au compte) sans être client Google ou Apple (vente forcée). L'UE a poussé les citoyens européens dans les bras des GAFAM, de force.
> Non pas obligé d'utiliser ces applis, je l'utilise sans l'appli que je n'ai jamais utilisé, ils sont obligés en théorie de vous envoyer un courrier papier avec un code dedans pour remplacer le code fourni par l'application si nécessaire.
>> Oui mais si 99,9% des gens rentrent dans ce système, à la fin cette solution alternative ne sera plus proposée. En pratique, c'est "obligé" d'utiliser l'appli car pour la contourner c'est fait pour être galère, décourageant. Bien d'accord. la solution pour moi c'est de sortir de ces banques privées mais ça reste compliqué aujourd'hui....

- Quelles sont les limites juridiques à l'utilisation de la reconnaissance faciale pour l'identification généralisée permanente dans l'espace public ? Rien ne peut entraver l'arrivée du « contrôle d'identité généralisé et permanent » ?

Vous avez oublier de parler de yunohost !!! ;) https://yunohost.org/#/ <<<<

- Est-ce qu'il y une réflexion au sein de la lQdN sur les conséquences individuelles pour les gens qui souffrent d'avoir consciences de tous ces sujets. Comme on peut souffrir d'éco-anxiété, est-ce qu'il y a pas des gens qui souffrent de surveillance-de-masse-anxiété ? Genre des gens qui sortent plus de chez eux parce qu'ils ont peur

des caméras de vidéo-surveillances partout...
La communauté infosec que je vois a plutôt tendance à déprimer dans son coin qu'autre chose, ce qui reste assez terrible, mais je ne connais pas de cas de personnes qui souffrent d'anxiété générale à cause de ça. Ce qui ne veut pas dire que ça n'existe pas.

lQdN est aussi financé par des entreprises. ... oui, mais dans la limite d'un don de 1000€, comme pour tout autre don :) Non, y'a des entreprises qui ont donné plus (c'est pas un reproche, juste il faut pas dire que y'a que des dons d'individus).

- que pensez vous du biohacking ? j'ai participé à un workshop, et c'était intéressant avec certaines parties un peu gadget, mais j'y ai perçu une sorte d'idéologie... vous connaissez le courant ?

-bon quel outil peut-être utilisé pour permettre la protection données sans mauvaise surprise du coup?

- vous avez pris connaissance des propositions des sénateurs "le crisis data hub"?

- Chiffré le disque dur c'est pas suffisant ?
Chiffrer le disque dur est nécessaire, mais pas suffisant. Ça ne protège que contre un cas précis : qqn cherche à accéder à votre ordinateur alors que celui-ci est éteint. S'il est allumé, les clés de déchiffrement sont (nécessairement) chargées quelque part dans l'ordinateur pour pouvoir accéder aux données sur le disque dur. Dans la majorité des cas, quand l'ordinateur est allumé elles sont chargées en mémoire vive et peuvent être extraites par un adversaire un peu qualifié (cf. https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9marrage_%C3%A0_froid ou simplement une faille dans l'OS qui déboucherait sur un accès admin / root, permettant d'extraire les clés). Malgré ces limites, il est nécessaire de le chiffrer ses machines : ça ne coûte rien et ça protège la machine quand elle est éteinte (encore une fois, avec certaines limites, mais bon, tout le jeu est de mettre assez de protections en place pour rendre les attaques difficiles ou trop coûteuses)

- Petite question qui peut paraître idiote, est-ce utile (nécessaire) de masquer la caméra de l'ordi pour éviter d'être surveillé à l'insu de son plein gré ?C'est une bonne pratique, et ça mange pas de pain
J'aurais tendance à dire que oui, je prend pour exemple une résidence étudiante où j'étais et où l'accès internet était collectif, un élève avait eu accès aux webcams des ordinateurs portables des autres étudiants.
Merci pour les réponses, mais si je suis la seule utilisatrice de mon ordi perso dans mon appart où je vis seule (avec ma chatte) est-ce que je cours un risque ? J'y connais pas grand chose, mais je pense que c'est une bonne chose de cacher sa webcam. Si on l'utilise, on peut simplement mettre un petit bout de post-it qui s'enlève facilement. OK merci Avec plaisir :) Perso, j'ai découpé un petit bout du collant d'un post-it que j'ai mis sur ma webcam d'ordi portable et de mon smartphone aussi (le côté tourné vers soi de la caméra du smartphone).
Le risque est surtout d'un accès à distance à son ordinateur, via une faille de sécurité dans Windows, MacOS ou Linux par exemple. Les RAT (remote access

tools) sont beaucoup utilisés pour espionner des femmes par une (petite) communauté de connards. Eva Galperin de l'EFF fait un travail remarquable sur les "stalkerware", les logiciels d'espionnage : https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/

Il y a un an, vous (LQDN) avez occupé une place importante dans la lutte contre la loi Sécurité globale, quel bilan en tirez vous? Plus globalement, quelles leçons tirez-vous de la période, quels objectifs/quelles priorités pour les mois à venir ? Quelles coopérations possibles avec les organisations de la société civile ?

Le groupe Sensibilisation de l'April travaille sur l'information du grand public pour le choix d'ordi et de téléphone utilisable directement sous un OS libre (dont /e/ par ex). Prochaine réunion ce jeudi 18 novembre.
https://wiki.april.org/w/Reunion_du_4_novembre_2021

est-ce que les pratiques de sousveillance type copwatching est une utopie ? aux usa et en France on a pas vu de différences les policiers ne sont pas plus condamnés ou moins violent ?

- calyx c'est le Linux Mint du téléphone ?
Je sais pas, j'espère pas, je suis pas fan de Linux Mint, j'ai jamais été convaincu par certains de leur choix en terme de sécurité. J'espère que c'est plutôt le Debian ou le Fedora du téléphone :) Mais en tout cas, ça semble être une bonne alternative à LineageOS (et surtout aux versions dégueulasses d'Android livrées par défaut dans la majorité des cas)

- question du chat | hjmp: Vers qui peut on se tourner si on est sous surveillance par une orga genre secte/mafia ?

- question difficile, comment la personne est-elle certaine d'être sous surveillance ? Si c'est réellement le cas, «?il faut aller voir la police?», avec toutes les énormes limites que ça implique. Sinon faites-moi signe sur Twitter ou par mail qu'on en discute pour quels sont les éléments qui laissent penser que c'est le cas - axel

- des sources viables pour apprendre a faire?

Je vais pas tout détailler ici mais vraiment regardez le fonctionnement de Briar pour les messageries, en terme de distribution de clés (publiques) ça n'utilise pas de serveur central ! contrairement à Signal, Whatsapp, Telegram... :
https://briarproject.org/
Olvid est pas mal aussi mais pas aussi poussé que Briar (https://briarproject.org/)

Bonsoir,
Que pensez vous de la sécurité des applications de gestion d'objets connectés?
j'ai acheté une ampoule connectée à 13€ que j'ai couplé avec Smart Life et IFTTT, car philips hue trop cher, et je ne me voyais pas me lancer dans le code de script avec un Arduino.
Globalement, la sécurité des objets connectés est désastreuse :) À moins que ça

vienne d'un constructeur qui fait des mises à jour logicielles régulières, partir du principe que l'objet est une passoire et que n'importe qui sur Internet peut y accéder / possiblement le contrôler. Le mieux est de créer un réseau secondaire séparé pour mettre en place un cloisonnement de ces objets et qu'ils ne puissent pas accéder aux restes des ordis, téléphones, imprimantes etc. de la maison, mais c'est déjà un truc assez avancé (cf. VLAN + point d'accès wifi secondaire, bref, pas évident)

https://bitcointv.com/w/eSXdVGYJGY77UjX5CNmq4b ? vidéo pour une comparaison sérieuse des différentes solutions de messageries instantanées.

Moteurs de recherche : Qwant est-il efficace en matière de protection des données ?
-merci & à la prochaine-
Merci beaucoup !
Merci aussi pour le document.