CYBER-SÉCURITÉ

Tour d'horizon

Blue Wave Software

Olivier Merlin

Les sujets

- Les grandes catégories de risques et leurs conséquences
- Les menaces et les vulnérabilités
- Les protections
- Du concret
- Le constat chez soi

Q&R interactives : n'hésitez pas à m'interrompre !

Vidéo : https://www.youtube.com/watch?v=tFaLCj4qBuc (source : EY France)

bws BLUE WAVE SOFTWARE

- Mon informatique ne marche plus/mon PC ne démarre plus, a brûlé/est noyée…
- J'ai perdu mes données (contacts, commandes, factures, contrats…)
- Mes données ont été exfiltrées ou piratées (GDPR 25/05/2018)
- J'ai perdu/on m'a volé mon PC/tablette/téléphone
- Mon informatique a servi à mener des attaques ou stocker des données illégales
- J'ai perdu de l'argent
- etc.

- Vidéo: https://www.youtube.com/watch?v=V4MPd5IsKyQ (source BigWheel)

- Est-ce tout ? Comment être sûr ? Réponse par l'analyse !
  - Impact-conséquence/fréquence-probabilité
  - Prévenir/réduire/transférer/accepter
  https://fr.wikipedia.org/wiki/Gestion_des_risques

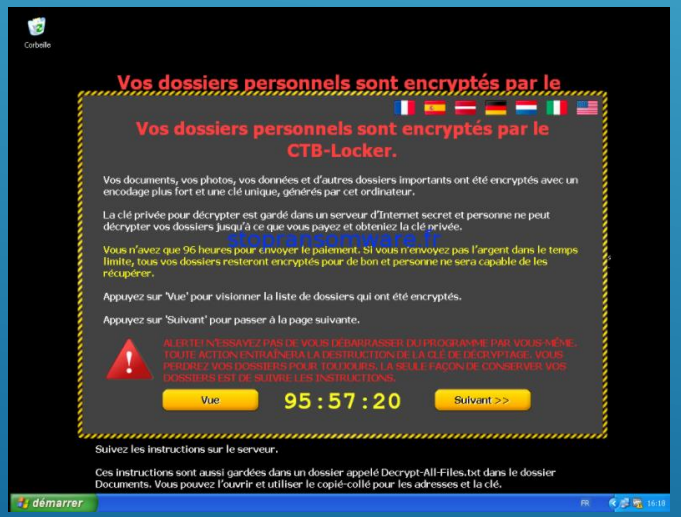
Gestion des risques

bws BLUE WAVE SOFTWARE

Les menaces

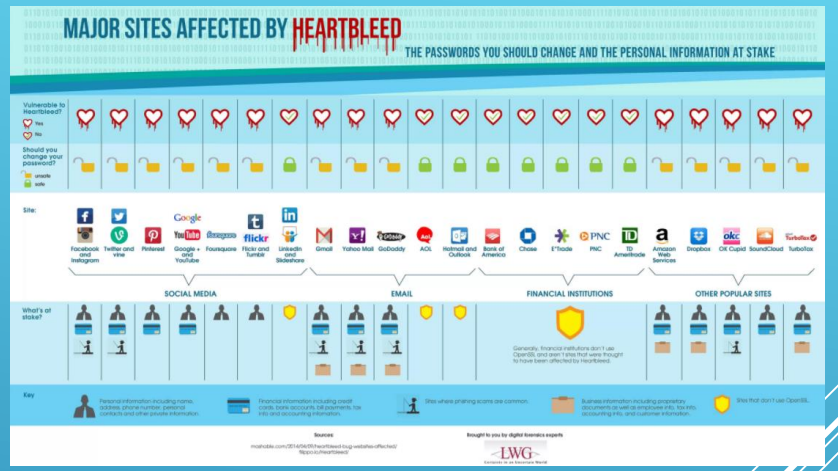
- ANSSI: déstabilisation/espionnage/sabotage/cyber-criminalité https://www.ssi.gouv.fr/particulier/principales-menaces/
- Déstabilisation: défiguration de site web, divulgations de données, déni de service…
- Espionnage: concurrence et Etats
- Sabotage: destruction (OIV, industries…)
- Cyber-criminalité: malware, rançongiciels/ransomware, phishing…

et plein d'autres…



Les vulnérabilités

- Vulnérabilités humaines
  - arnaque à la présidente (et autres spear phishing, les plus dangereux)
  - rôle des réseaux sociaux
  - faux sites web, pas de https
  - etc…
- Vulnérabilités informatiques:
  CVE (Common Vulnerabilities and Exposure)
  - la plupart du temps un bug de programmation rend un système d'exploitation ou un logiciel vulnérable
  - « Zero-day » : on ne la connaît pas encore !



exemple vulnérabilité « EternalBlue » : « WannaCry » (ransomware 12/05/2017) en profite, « a priori » vulnérabilité dérobée à la NSA par le groupe de hackers Shadow Brokers, la NSA prévenant alors Microsoft, alors que le patch MS17-010 de la CVE-2017-0144 par Microsoft date du 14/03/2017 – qui émet même des patches XP et Windows 2003, systèmes plus supportés (attention aux OS plus supportés !)

exemple vidéo BlueBorne:
Windows : https://www.youtube.com/watch?v=QrHbZPO9Rnc (source Armis)
Android : https://www.youtube.com/watch?v=Az-l90RCns8 (source Armis)

bws BLUE WAVE SOFTWARE

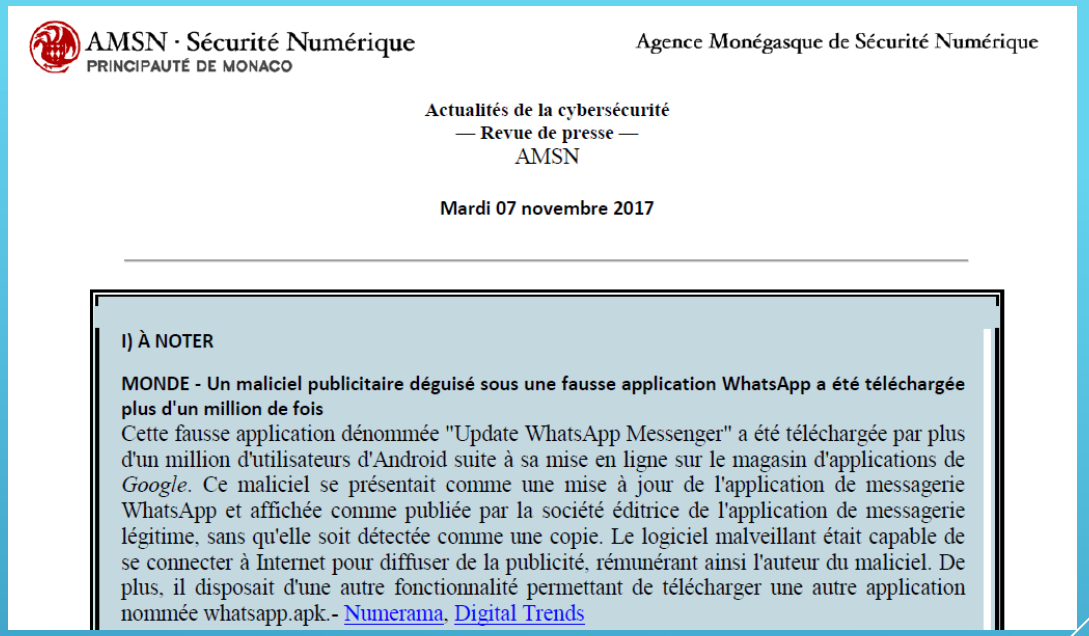
Les protections

- Être constamment A JOUR ! (on limite ainsi beaucoup les risques et la surface exposée) Certains outils permettent de savoir exhaustivement tout ce qui n'est pas à jour.
- Avoir des passerelles/firewall intégrant des compléments de ces outils, genre firewall UTM = virus/malware/botnet/ips/spam, tout en comprenant bien les limites de ce type de sécurité périmétrique: **c'est le poste final (EndPoint) qui compte en définitive !**
- Des éléments basiques: un anti-virus, soit, mais à jour et complété d'un anti-malware qui couvrira d'autres menaces, une bonne gestion des comptes et droits informatiques, une surveillance continue…
- Avoir des sauvegardes régulières (3-2-1) voire un plan de reprise d'activité/site séparé
- Chiffrer les communications (https) mais aussi les outils mobiles (totalement ou partiellement), voire chiffrer sur les PC et/ou serveurs et les mails
- Faire des sessions de sensibilisation auprès des utilisateurs (reconnaître un mail bizarre et demander, s'arrêter de surfer si le https hurle, ne pas répondre au téléphone en disant tout sur tout, protéger ses mots de passe grâce à un gestionnaire spécifique et/ou utiliser de l'authentification forte…)
- Vérifier si l'on dépend d'une règlementation, demander des conseils aux spécialistes, consulter les recommandations de l'ANSSI/Clusif/…

bws BLUE WAVE SOFTWARE

- S'abonner à leur bulletin (amsn@gouv.mc)
- Type de news:
  - Apple : un bug sur la dernière version MacOs affiche le mot de passe en clair quand on clique sur le bouton « Afficher l'indice »
  - Croissance de 2500% sur le rançongiciel
  - Faille critique WPA2 : des pirates peuvent profiter de la vulnérabilité KRACK (octobre 2017) pour écouter les réseaux sécurisés (Krack serait connu de la NSA depuis 2010 – source Snowden)

  etc.



AMSN · Sécurité Numérique
PRINCIPAUTÉ DE MONACO

Agence Monégasque de Sécurité Numérique

Actualités de la cybersécurité
— Revue de presse —
AMSN

Mardi 07 novembre 2017

I) À NOTER

MONDE - Un maliciel publicitaire déguisé sous une fausse application WhatsApp a été téléchargée plus d'un million de fois
Cette fausse application dénommée "Update WhatsApp Messenger" a été téléchargée par plus d'un million d'utilisateurs d'Android suite à sa mise en ligne sur le magasin d'applications de *Google*. Ce maliciel se présentait comme une mise à jour de l'application de messagerie WhatsApp et affichée comme publiée par la société éditrice de l'application de messagerie légitime, sans qu'elle soit détectée comme une copie. Le logiciel malveillant était capable de se connecter à Internet pour diffuser de la publicité, rémunérant ainsi l'auteur du maliciel. De plus, il disposait d'une autre fonctionnalité permettant de télécharger une autre application nommée whatsapp.apk.- Numerama, Digital Trends

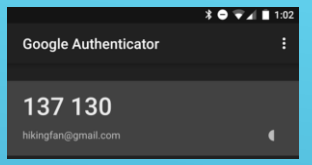
AMSN

http://www.gouv.mc/Gouvernement-et-Institutions/Le-Gouvernement/Departement-de-l-Interieur/Agence-Monegasque-de-Securite-Numerique

bws BLUE WAVE SOFTWARE

Conseils pratiques

- Utiliser un gestionnaire de mots de passe (local = KeePass…, cloud = Lastpass/Dashlane…) avec mots de passe complexes
  (ne stockez pas dans les navigateurs, verrouillez votre poste)
- Partout où c'est possible, mettre une authentification forte/double (2FA = Google authenticator…) : https://twofactorauth.org/
- Utiliser le Cloud ? oui, mais avec authentification forte et au besoin avec chiffrement (BoxCryptor pour Dropbox, OneDrive…)
- Se connecter à des réseaux publics Wi-Fi non sécurisés: à éviter dans la mesure du possible
- Doute sur un fichier ou url ? VirusTotal : https://www.virustotal.com/fr/
- Nettoyer ses traces si nécessaire: CCleaner
- Victime de ransomware : ne pas payer, ne rien faire, appeler un spécialiste, aide sur https://www.nomoreransom.org/fr/index.html
- Vérifier sur « Have I been pwned? » https://haveibeenpwned.com/
- Se méfier des objets IoT : on isole !



bws BLUE WAVE SOFTWARE

- Savoir où l'on en est (culture d'entreprise et soi-même) aussi bien à un moment T que dans le temps
- Se faire surveiller/auditer régulièrement:
  - outils de tests de vulnérabilités récurrents
  - sensibilisation des utilisateurs (campagnes des tests)
  - audit de son infrastructure, certification ISO 27001…
- En cas de détection de vulnérabilité, de mauvais comportement ou d'incident, avoir des procédures prêtes, des gens formés ou un contrat de service
- Suis-je équipé pour gérer ça en interne ou dois-je faire appel à des spécialistes ?
- Attaques/incidents: se rapprocher de l'AMSN, porter plainte auprès de la Sûreté Publique…

Où en suis-je ?

bws BLUE WAVE SOFTWARE

On n'est jamais sécurisé à 100% !

vidéo : https://www.youtube.com/watch?v=PLqJiEMpZfQ

MERCI POUR VOTRE ATTENTION !

olivier.merlin@bluewave.mc

bws BLUE WAVE SOFTWARE