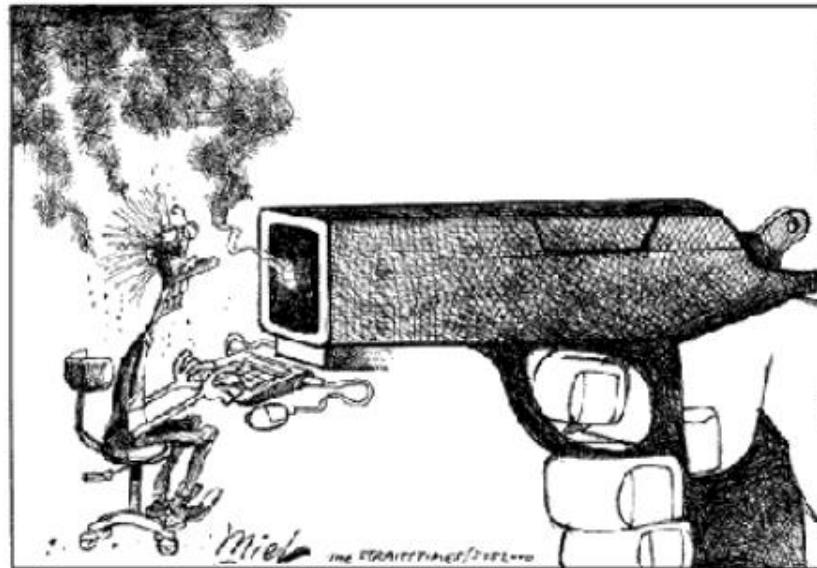


Etat des lieux des menaces fin 2018

A quoi s'attendre en 2019 ?



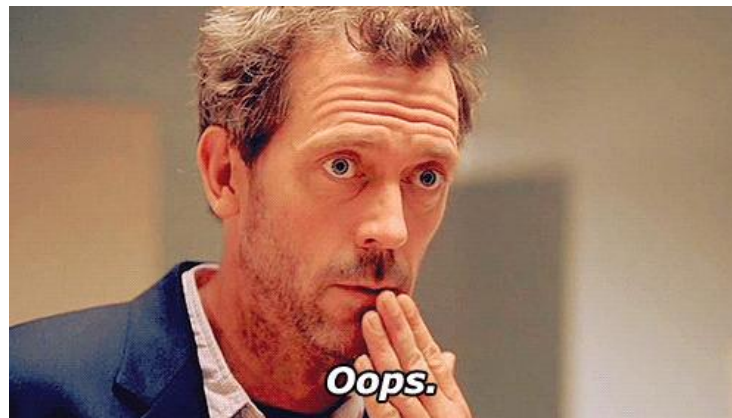
Patrick CHAMBET – RSSI
Métropole Nice Côte d'Azur
CLUSIR PACA

Sommaire

1. *Pourquoi sont-ils si méchants ?* Rappels sur les profils d'attaquants
2. Les principales attaques en 2018
3. Le maître mot: sensibilisation
4. Perspectives pour 2019

En synthèse

- Il y a 2 sortes d'entreprises:
 - celles qui ont déjà été attaquées
 - celles qui ont déjà été attaquées... et qui ne s'en sont toujours pas rendu compte !



Les profils d'attaquants

- Le hacker « canal historique »
 - Type: barbu, geek, nerd 😊, ... « white hat »
 - But: pour le prestige, améliorer la qualité des logiciels
 - Espèce: en voie de disparition
- Le « hacktiviste »
 - Type d'attaques: défiguration de sites Web par ex.
 - But: faire passer un message, souvent politique (ex: les Anonymous)
 - Espèce: stable

Les profils d'attaquants

- Le cyber-délinquant
 - Type: opportuniste, de plus en plus organisé, voire mafieux
 - But: gagner de l'argent / survivre
 - Espèce: invasive, propagation exponentielle
- Le cyber-terroriste
 - Type d'attaque: action à retentissement important
 - But: marquer les esprits, déstabiliser
 - Espèce: en expansion



Les profils d'attaquants

- L'état étranger
 - Type: agents officiels, soldats/équipes spécialisés
 - But: déstabiliser un état, paralyser ses services essentiels, préparation furtive d'un futur (cyber)-conflit
 - Espèce: en expansion
- Les cyber-mercenaires
 - Type: groupes d'attaquants liés à un état ou à une organisation, mais agissant seuls, spontanément
 - But: faire passer un message, déstabiliser, nuire au fonctionnement d'un état
 - Espèce: en expansion

Les différents types d'attaques

- Attaques réseau
 - En baisse, sauf les dénis de service, en hausse
- Attaques applicatives
 - Toujours actives
- Attaques sur l'interface chaise-clavier (l'humain)
 - En explosion depuis quelques années !



Attaques humaines

- Ce sont les attaques les plus courantes et les plus innovantes (quoi que...) depuis quelques années
- Le plus souvent par mail
 - Le mail constitue maintenant la principale porte d'entrée dans les entreprises
- Spam de type « arnaque »
 - « J'ai un gros héritage que j'aimerais faire revenir en France... »
➔ ne diminue pas !
- Ingénierie sociale / arnaque « au Président »
 - Par mail / par téléphone
 - Compétence très pointue des arnaqueurs
 - Conséquence: faillites d'entreprises



Attaques humaines

- Phishing
 - Principe: se faire passer pour une entreprise légitime
 - Soutirer des informations sensibles
- Virus / cheval de Troie
 - Sous forme de pièce attachée
 - Utilisation d'une vulnérabilité du client mail ou non
- Ransomwares
 - Sous forme de pièce attachée
 - Ne se propage pas... jusqu'à WannaCry (ver + ransomware) !

Ransomware

Cryptorbit

YOUR PERSONAL FILES ARE ENCRYPTED

All files including videos, photos and documents, etc on your computer are encrypted.

Encryption was produced using a **unique** public key generated for this computer. To decrypt files, you need to obtain the **private** key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; **the server will destroy the key after a time specified in this window.** After that, nobody and never will be able to restore files

In order to decrypt the files, open site **4sfxtgp53imlvzk.onion.to/index.php** and follow the instructions.

If **4sfxtgp53imlvzk.onion.to** is not opening, please follow the steps below:

1. You must download and install this browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After installation, run the browser and enter the address: **4sfxtgp53imlvzk.onion.to/index.php**
3. Follow the instructions on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.



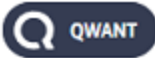
Ransomware



Attaques humaines

- Plus récent
 - Chantage au faux virus
 - Message d'erreur bloquant avec numéro de tel à appeler
 - Source: annonces Google par ex.
 - But: faire payer ou installer un malware à distance
 - Chantage à la fausse vidéo... mais au vrai mot de passe !
 - Mail avec message de chantage agressif et affichage de l'un de vos vrais mots de passe en clair
 - Mot de passe récupéré dans les bases de comptes piratés
 - LinkedIn en 2016, Yahoo!, Adobe, ...
 - Ne pas répondre
 - Changer les mots de passe de tous vos comptes piratés... et des comptes où vous avez réutilisé ces mots de passe (**c'est mal !**)
 - Voir: <https://haveibeenpwned.com>

Chantage au faux virus




SUR LE WEB

Période ▾

Meteo France - Voir 14 Jours à L'avance


ANNONCE www.meteofrance.com

Trouvez les meilleurs endroits pour obtenir les prévisions les plus précises.

Meteo France - Cliquez pour entrer | gonline.icu


ANNONCE gonline.icu/Meteo France

Obtenez un accès meilleur et plus facile à vos sites préférés. Va ici.

Annonces par Microsoft ([Confidentialité](#))

PREVISIONS METEO FRANCE - Site Officiel de Météo-France - Prévisions gratuites ...


meteofrance.com/accueil

PREVISIONS METEO FRANCE - Site Officiel de Météo-France - Prévisions gratuites à 15 jours sur la France et à 10 jou...

Météo-France


fr.wikipedia.org/wiki/Météo-France

Météo-France, établissement public administratif, est le service officiel de la météorologie et de la climatologie en **France**. À ce titre, il exerce le...

Carte de vigilance Météo-France


vigilance.meteofrance.com

Carte de vigilance **Météo-France**

Chantage au faux virus

*** STOP: 0x0000000c (0x00000000, 0xEB71092F, 0x00000008, 0xC0000000)
BAD_WEB_ADDRESS_NOT_HANDLED *** Address EB662040 at EB660000

CPUID:Genuine Intel 6.3.3 irq:1f SYSVER 0xF0000565

Dll Base	DateStmp	- Name
80100000	336546bf	- ntoskrnl.exe
80000100	334d3a53	- atapi.sys
802aa000	33013e6b	- epst.mpd
802b9000	336015af	- CLASS2.SYS
802ba000	33d844be	- huml.sys
f9318000	31ec6c8d	- Floppy.SYS
f9468000	31ed868b	- KSecDD.SYS
f9358000	335bc82a	- i8042prt.sys
f947c000	31ec6c94	- kbdcass.sys
f9370000	33248011	- VIDEOPORT.SYS
f9490000	31ec6c6d	- vga.sys
f90f0000	332480d0	- Npfs.SYS
a0000000	335157ac	- win32k.sys
fe0c9000	335bd30c	- Fastfat.SYS
fe108000	31ec6c9b	- Parallel.SYS
f9050000	332480ab	- Serial.SYS

Ne pas redémarrer ou redéfinir les options de récupération dans le panneau de configuration. Contactez immédiatement le support technique au 09 75 18 68 09.

Veillez s'il vous plait appelez le 09 75 18 68 09

Confirmation de Navigation

Le problème est causé par une activité inhabituelle effectuée sur cette machine.

Code erreur : 01AAT

Appelez le support technique au 09 75 18 68 09 et communiquez le code d'erreur au technicien.

êtes-vous sur de vouloir quitter cette page?

Quitter
Rester

Message de la page Web

*** NE PAS REDEMARRER VOTRE ORDINATEUR ***

Un virus à été détecté sur votre ORDINATEUR.

Les infections détectées indiquent plusieurs téléchargements récents frauduleux sur l'ordinateur qui ont ensuite créés des problèmes CRITIQUES.

Contactez immédiatement le support technique au 09 75 18 68 09 et indiquez le code erreur suivant au technicien afin de réparer votre ordinateur: 01AAT.

OK

DETECTION DES MENACES POTENTIELLES SUR VOTRE ORDINATEUR

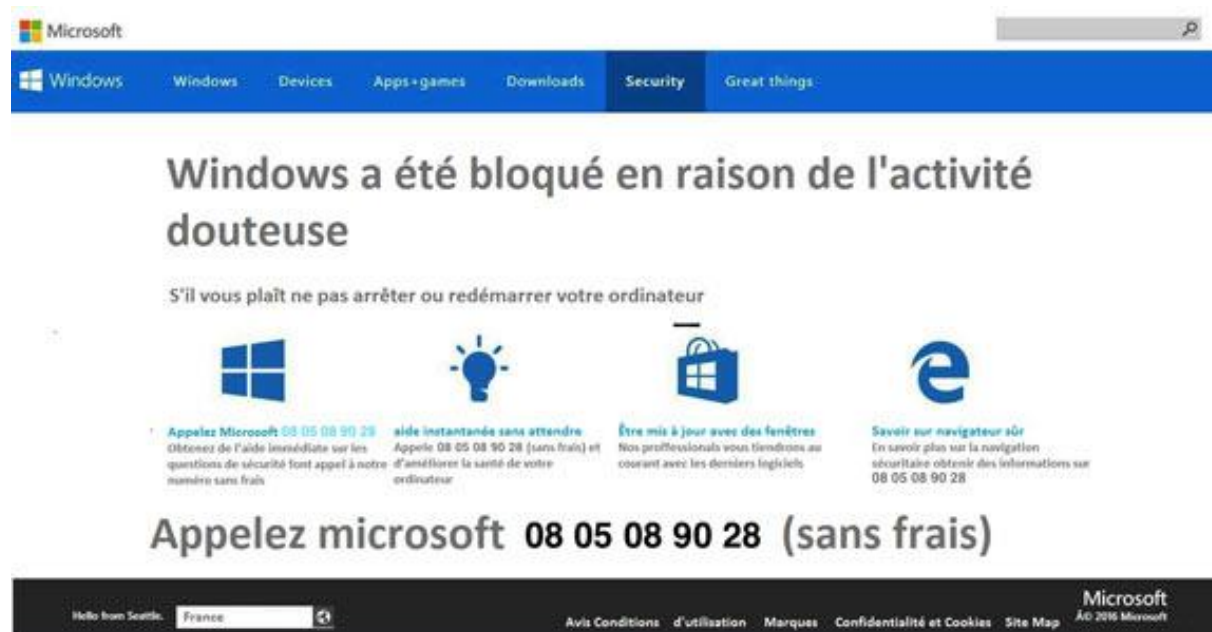
Essential de sécurité ne sont pas fiables pour bloquer le virus. Détection des menaces potentielles qui pourraient compromettre votre vie privée ou d'endommager votre ordinateur.

Code d'erreur: 8x92344cc, impossible d'installer les mises à jour.

Système peut être l'usage nocif comme a-été détecté le virus.

CONTACTER SUPPORT 09 75 18 68 09

Chantage au faux virus



Le maître mot: sensibilisation

- Il existe des moyens techniques de protection
 - Anti-spam / anti-malware de messagerie + Web
 - « Sandbox »
 - Endpoint Protection
 - Mises à jour des logiciels clients
 - Navigateur, client mail, Flash, Java, lecteur PDF, ...
- Mais il est indispensable de sensibiliser les utilisateurs
 - Formation
 - Animations / sensibilisations
 - Voire campagne de phishing interne
- Et rien ne remplace le fait de se faire avoir une fois !
 - Quand on a perdu une fois toutes ses photos persos, on fait attention par la suite... (c'est malheureux mais c'est humain)

Sensibilisation



- C'est lui qui a infecté tout le réseau ?
- Oui, c'est lui qui a double-cliqué sur la pièce attachée...

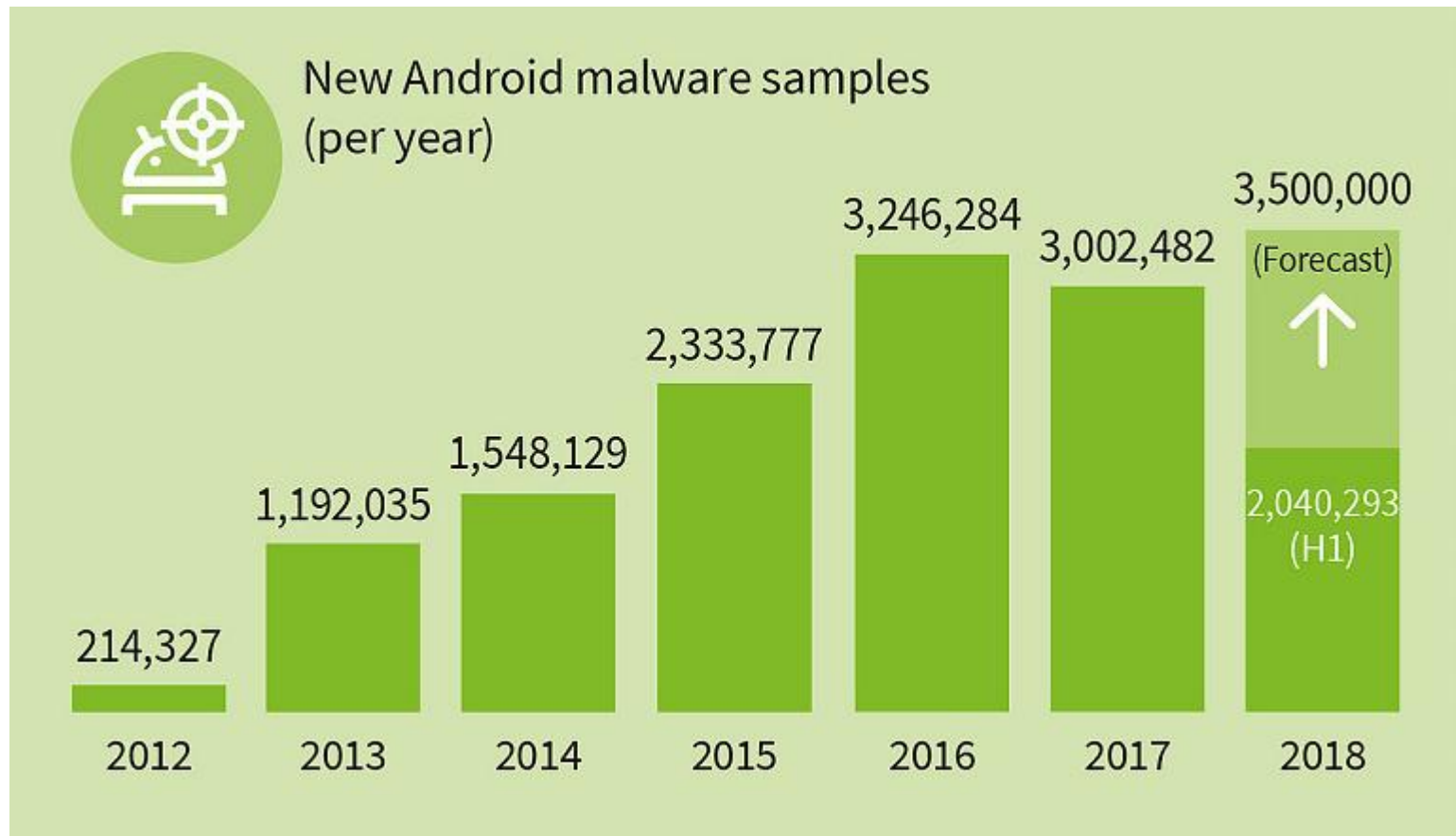


Perspectives 2019

- Les « nouvelles » cibles
 - Les systèmes industriels (SCADA)
 - Attention aux OIV
 - Cf intervention de G. Poupard, DG de l'ANSSI: « il va y avoir des morts... »
 - Les systèmes de santé
 - Les objets connectés
 - Notamment personnels
 - Les nouveaux systèmes à adoption de plus en plus large
 - Apple, Linux : virus, malwares « in the wild »
 - Nouveaux vers à prévoir (cf Mirai, ampoules Philips, ...)
- Nouvelles attaques humaines à prévoir
 - Vont tenir compte de l'évolution des usages
 - Mais aussi de l'augmentation de la sensibilisation des utilisateurs
 - Inventivité et motivation sans limite des attaquants dont c'est le métier / le moyen de subsistance / de rester en vie

Perspectives 2019

- Attaques sur les smartphones



Source: GData

Perspectives 2019

- Attaques sur les smartphones (suite)
 - Ex. de ver sur Android: ADB.Miner
 - Cherche à se connecter au port TCP 5555 du smartphone et de ses voisins pour accéder à l'interface ADB (mode débogage)
 - Mode désactivé en général, mais parfois laissé actif chez certains constructeurs (en Asie par exemple)
 - Permet d'avoir un accès root et d'installer un cryptominer, puis de se diffuser automatiquement
 - « Semi ver » seulement, car en général un message de confirmation est demandé à l'utilisateur



Conclusion

- Les attaques sont une donnée de base: elles arrivent tous les jours et vont encore augmenter en nombre et en sophistication
- Les attaques humaines sont toujours efficaces et ne vont donc pas disparaître de sitôt
- Il faut se préparer à l'avance au niveau proactif et réactif: se protéger, savoir les détecter, être capable de réagir quand elles arrivent
- Les SCADA et les objets connectés ouvrent de nouvelles perspectives pour les attaques à venir



Questions ?