CLUSIR
Aquitaine

#MacronLeaks
#WannaCry

RSSIA2017
Bordeaux, 16 juin 2017

Hervé Schauer
<Herve.Schauer@hsc-labs.com>
@Herve_Schauer

Plan

- #Macronleaks
- #Wannacry
- Conclusion

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#MacronLeaks : Annonces

- 5 mai 2017, sur *tweeter*, avant le second tour élections présidentielles du 7 mai
- Dans la fuite :
  - Ajout de documents falsifiés grossièrement
    - Méta-données en russe
  - Ajout d'un dossier entier venant d'ailleurs
- Utilisation de faux ne venant pas de la fuite
- Annonces
  - `http://www.liberation.fr/planete/2017/06/02/les-macronleaks-dans-le-brouillard-de-la-guerre-informationnelle_1574139`
  - `http://www.slate.fr/story/145221/le-macronleaks-est-une-fakenews`

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#MacronLeaks : Réactions

- Mounir Mahjoubi réagit
  - 5 boites de messagerie volées
  - Attribut la fuite au FN
  - Expliques que LREM a subit des attaques sophistiquées

> *"Une fachosphère hyper organisée et soutenue par des forces et des organisations étrangères"*
>
> **— Mounir Mahjoubi**
> **responsable de la campagne numérique d'En marche !**
> *à franceinfo*

- Explique qu'il a leurré les pirates en mettant à leur disposition de fausses informations « Il s'agit du brouillard » « on a créé plusieurs dizaines de milliers de faux » « on a zéro moyens »

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#MacronLeaks : Réactions

- New York Times souligne l'ingéniosité de l'équipe de campagne
  - Miracles de la communication faite par un publicitaire !

- Réactions
  - https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html
  - http://www.francetvinfo.fr/politique/emmanuel-macron/video-mounirmahjoubi-patron-de-lacampagne-numerique-d-emmanuel-macron-le-macronleaks-ca-pue-la-panique_2180759.html
  - http://www.usinenouvelle.com/article/comment-en-marche-a-tente-de-prevenir-le-macronleaks.N538974

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#MacronLeaks : Analyses

- Aimeriez-vous que vos archives de messagerie soient publiées ?
- Campagne totalement financée par la « finance »
  - Notamment à Londres
- Rappel : l'ANSSI avait convoqué les partis
- Analyses du contenu des documents
  - `http://www.liberation.fr/elections-presidentielle-legislatives-2017/2017/05/11/comment-en-marche-a-resolu-sa-question-de-fonds_1568975`
  - `http://www.mediapart.fr/journal/france/210517/macron-leaks-les-secrets-dune-levee-de-fonds-hors-norme`

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#MacronLeaks : Attribution

- Mai : APT28, russes, extrême-droite, etc
- Juin : pas de traces russes
- Guillaume Poupard, ANSSI : attaque basique
- Aucun parallèle possible avec le cas américain
- Attribution
  - `http://www.lemonde.fr/pixels/article/2017/06/02/macronleaks-1-enquete-pointe-vers-un-piratage-simple-et-generique_5137945_4408996.html`

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#WannaCry : Introduction

- WannaCrypt0r
- Rançongiciel
- Vers
  - MS17-010
  - Faille utilisée par la NSA
  - ShadowBrokers
  - Port tcp/445 SMB
- Souvenez-vous de Blaster en 2003
  - Qui a fait des morts...

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#WannaCry : Annonces

- Vendredi 12 mai
  - Hopitaux anglais (NHS)
  - Telefonica
  - Nouvelles alarmantes dans la presse grand public
- Samedi 13 mai (jour d'ESIEA Secure Edition)
  - BFMTV : Renault est touché
  - Europol : cyberattaque d'un niveau sans précédent
- Dimanche 14 mai
  - Journaux de 20h
  - BFMTV : usine Renault de Douai arrêtée lundi
- Lundi 15 mai
  - « Attention il va y avoir des répliques ! »

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#WannaCry : Annonces

- Annonces alarmantes :
  - https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack
  - https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today
  - https://www.us-cert.gov/ncas/alerts/TA17-132A
  - https://isc.sans.org/forums/diary/Massive+wave+of+ransomware+ongoing/22412/
  - http://blog.talosintelligence.com/2017/05/wannacry.html
  - http://www.bfmtv.com/international/cyberattaque-un-logiciel-de-rancon-frappe-des-dizaines-de-pays-1162889.html

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#WannaCry : Fonctionnement

- V 2.0 ?
  - Ou 0.2 ?
- Diffusion très très très faible
  - Dizaine d'entreprises en France
- Pas d'hameçonnage
    - Sauf un CERT qui a confondu avec le rançongiciel Jaff, similaire à locky
- Uniquement port TCP/445 (SMB)
  - A partir de Windows Server 2012 et Windows 10, 445 coupé par défaut
  - Chez vos opérateurs, coupé par défaut dans le sens internet → client
    - Ainsi aucune victime grand public
  - Hébergeurs/Prestataires d'Infonuagique également

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#WannaCry : Fonctionnement

- Ver orienté entreprises
  - Scan du réseau local d'abord
- Infection via
  - PC infecté sur un réseau non-protégé connecté à Internet, connecté ensuite sur le réseau local de l'entreprise
  - VPN depuis un PC infecté vers un serveur interne
    - Contournant les règles de protection périmétrique filtrant 445

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#WannaCry : OS victimes

- Portrait type des machines infectées et vulnérables réalisé par les pots de miel d'OVH
  - Surtout Windows Server 2008

OS Version	%	OS Category	%
Hyper-V Server 7601 Service Pack 1	1,2%	Hyper-V Server	1,2%
Windows 7 Enterprise 7601 Service Pack 1	0,3%	Windows 7	3,5%
Windows 7 Home Premium 7600	0,5%		
Windows 7 Professional 7601 Service Pack 1	0,7%		
Windows 7 Ultimate 7601 Service Pack 1	1,9%		
Windows 8.1 Pro 9600	0,3%	Windows 8	0,3%
Windows Server 2003 3790 Service Pack 1	0,3%	Windows Server 2003	0,3%
Windows Server 2008 R2 Datacenter 7600	0,5%	Windows Server 2008	94,1%
Windows Server 2008 R2 Datacenter 7601 Service Pack 1	4,3%		
Windows Server 2008 R2 Enterprise 7600	15,7%		
Windows Server 2008 R2 Enterprise 7600 Service Pack 1	0,3%		
Windows Server 2008 R2 Enterprise 7601 Service Pack 1	18,8%		
Windows Server 2008 R2 Standard 7600	6,8%		
Windows Server 2008 R2 Standard 7601 Service Pack 1	45,9%		
Windows Web Server 2008 R2 7600	0,3%		
Windows Web Server 2008 R2 7601 Service Pack 1	1,4%		
Windows Server 2012 R2 Standard 9600	0,5%	Windows Server 2012	0,5%

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#WannaCry : Arrêt

- « *Killswitch* »
  - Mécanisme d'arrêt du rançongiciel
  - Propagation stoppée par l'achat du domaine
  - Technique habituelle de détection de l'exécution en bac à sable
    - Vérification de l'inexistance d'un domaine
      - Si sur internet : le domaine n'existe pas
      - Si dans un bac à sable : simulation de réponse positive
    - Normalement le nom de domaine aurait du être aléatoire – pas le cas de WannaCry

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#WannaCry : Fonctionnement

- Sébastien Mériot, OVH, un *must read*
  - `https://www.ovh.com/fr/blog/wannacry-ransomware-sechez-vos-larmes-mais-restez-prudents`

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#WannaCry : Pas le seul !

- Adylkuzz a utilisé MS-17010 pour miner une cryptomonnaie (Monero) avant WannaCry
  - Evitant WannaCry par la suite
- Pleins de variantes
  - Corrigeant les lacunes de WannaCry
- Attention, toute machine infectée a aussi la porte dérobée DoublePulsar donc reste vulnérable

- Microsoft a publié un correctif pour Windows XP
  - C'était vendu des millions de $ avant WannaCry...

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#WannaCry : Enseignements

- Renault à Douai
  - Repris inlassablement par toute la presse, sans vérification
  - Source initiale semblerait être un syndicaliste
  - Retours contradictoires du personnel de Renault
  - Maintenance annuelle était ce week-end des 13-14 mai
- Victimes françaises
  - « grosses PME », ou filiales de groupe indépendantes
- Application des correctifs de sécurité
  - Ce qui était impossible, justifié comme impossible avec des dizaines de courriels, a été realisé en un week-end
- Exercice de gestion de crise pour tous
  - Pour un incident qui n'a pas eu lieu, mais pour prévenir qu'il arrive

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

#Wannacry : Attribution

- Attribution
  - A la Corée du nord par les USA
- Wannacry était-il un prototype ?
  - Sorti trop tôt par erreur ?
  - Seulement $140000 de récoltés
    - Ridicule comparé à ce qui était possible
- Attribution
  - `http://www.latribune.fr/technos-medias/informatique/wannacry-la-cyberattaque-mondiale-attribuee-a-la-coree-du-nord-par-la-nsa-740169.html`

Copyright Hervé Schauer Consultants 1989-2017 - Reproduction Interdite

Conclusion

- Evènements grand public, et communications fausses, mais effet **très positif** !
  - Sensibilisation grand public
  - Prise de conscience de certains dirigeants des risques numériques
    - Gestion de crise
    - Budgets & moyens humains
  - Preuve des capacités insoupçonnées des opérationnels
  - Entrainement à la gestion de crise

Copyright Hervé Schauer Consultants 2000-2015 – Reproduction interdite

Questions ?

www.hsc-formation.fr

<Herve.Schauer@hsc-labs.com>
@Herve_Schauer

Copyright Hervé Schauer Consultants 2000-2015 – Reproduction interdite