Thierry Matusiak
Architecte Division Sécurité IBM
Membre actif du CLUSIF
thierry_matusiak@fr.ibm.com
LinkedIn : https://fr.linkedin.com/in/thierrymatusiak

Panorama de la cybercriminalité

Club de la sécurité de l'information français

CLUSIF

Panorama de la cybercriminalité année 2017

Paris, 18 janvier 2018

- Extrait pour le séminaire CyberSécurité Aristote -

- 1er octobre 2018 -

PanoCrim 2018 aura lieu le 10 Janvier 2019

#PANOCRIM

Club de la sécurité de l'information français

Présentation du CLUSIF

- **Association de professionnels de la sécurité de l'information**

Lieu d'échange, permettant de mettre en commun expertises et réflexions au service d'une SSI efficace

- **Les activités de l'association**
  - des groupes et Espaces de Travail
  - des publications
  - des conférences thématiques
  - des ateliers fournisseurs sur le grill
  - un exercice de Cyber-Crise (ECRANS 2017)

Pour plus d'information : clusif@clusif.fr

Panorama 2017 – synthèse pour Aristote

- Attaques destructives
- Attaques via des tierces parties
- Vecteurs d'attaques innovants : le Cloud et l'IoT
- Bitcoin & Co : l'envol des prix attire les cybercriminels

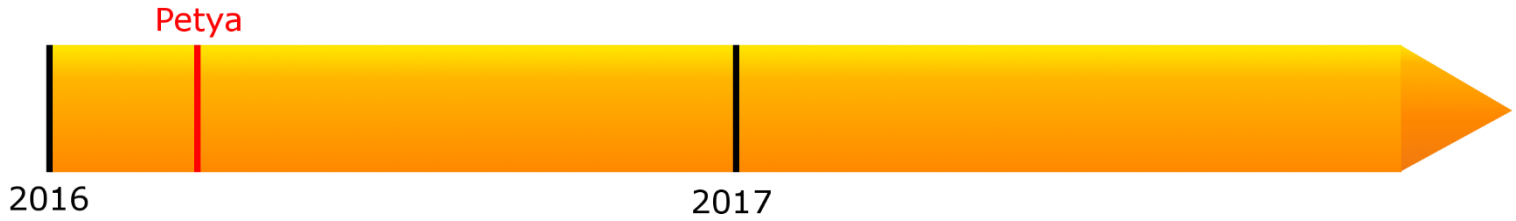
- En janvier, on a également abordé :
  - La gestion de crise et ses limites
  - Elections et cyber, les enjeux géopolitiques
  - Rançon : payer ou ne pas payer ?
  - Ils ont été arrêtés : le Darknet mais pas que…
  - Les sujets émergents

CLUSIF

Attaques destructives

Petya

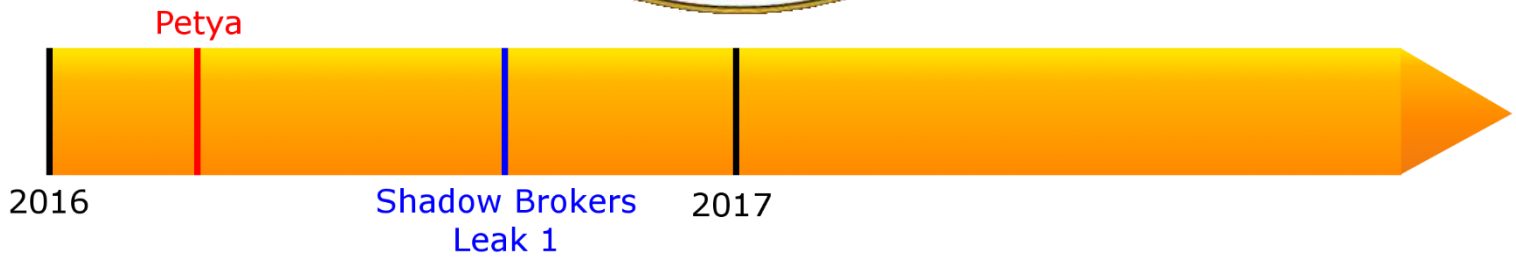

You became victim of the PETYA RANSOMWARE!
The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.
PRESS ANY KEY!
You became victim of the GOLDENEYE RANSOMWARE!
The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.
PRESS ANY KEY!


Petya
2016
2017

Petya, les prémices

- Mars 2016 : Apparition d'un nouveau type de rançongiciel
  - Stratégie de plus bas niveau que les rançongiciels précédents (Locky, Cerber, …)
- Attaques par spear-phishing qui ciblent l'Allemagne
  - Délivré par mail de motivation contenant un lien vers un Dropbox
  - Exécutable malveillant hébergé sur le Dropbox
- 4 versions successives de plus en plus matures
  - Red Petya, Green Petya, Green Petya patched, Goldeneye
  - Ajout d'un chiffrement haut niveau (Mischa) dès Green Petya
- Failles rapidement découvertes pour Red Petya et Green Petya
  - Récupération de la clé privée en mémoire immédiatement après l'infection
  - Découverte de la clé privée par force brute (faille dans l'algorithme SALSA20)
- Clé privée permettant le déchiffrement divulguée le 5 juillet 2017

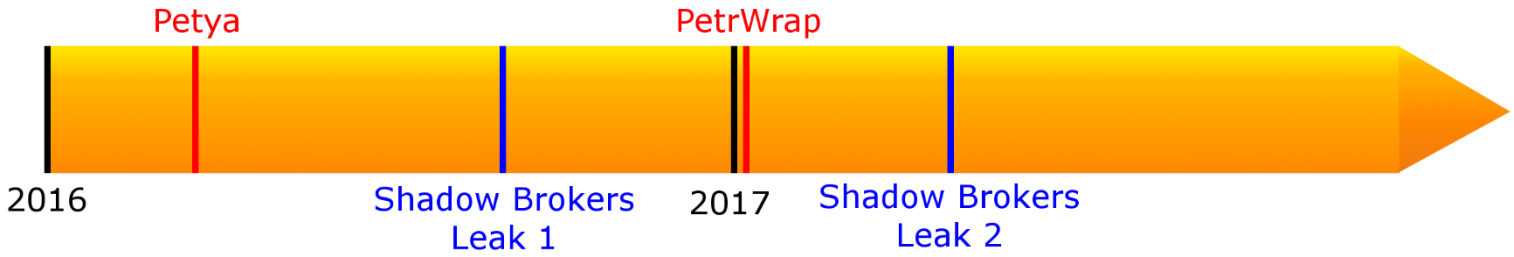
Shadow brokers vs. Equation group



Shadow brokers vs. Equation group

- Equation Group :
  - Cyber espionnage de haut niveau
  - Supposé être lié à la NSA
  - Auteur de nombreux exploits 0-day, portes dérobées ou troyens sur des logiciels et systèmes d'exploitation reconnus depuis 2001
- Shadow brokers :
  - Russes (hypothèse de E. Snowden) ou Américains (hypothèse de S.Argamon)
  - Infiltrés à la NSA (hypothèse d'anciens de la NSA)
- 13 août 2016 : Les Shadow brokers mettent en téléchargement libre des outils d'espionnage et de piratage volés à la NSA
  - Rapidement identifiés comme authentiques, mais pour la plupart obsolètes
  - Mise aux enchères des « meilleures armes informatiques » pour 1 million de Bitcoins

Shadow brokers vs. Equation group

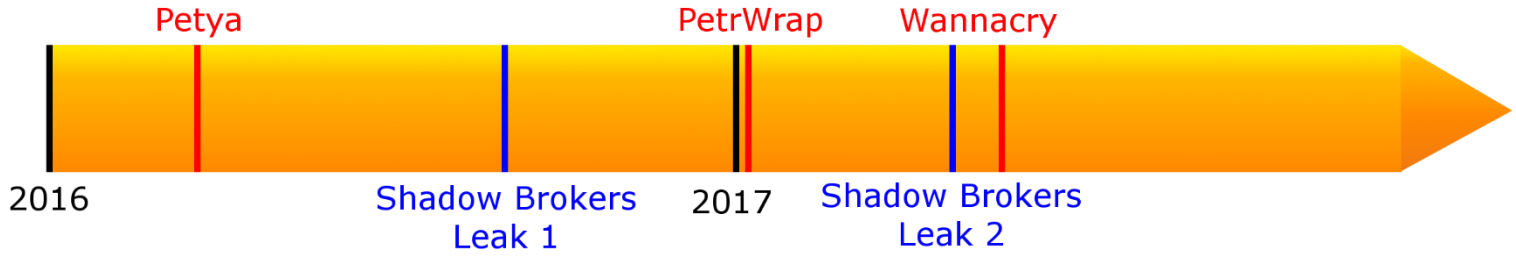


Shadow brokers vs. Equation group

- 8 avril 2017 : Les Shadow brokers expriment leur mécontentement face à la politique de D. Trump
- 14 avril 2017 : Publication de nouveaux outils dérobés à la NSA
  - Outils d'espionnage de SWIFT (peut-être utilisés par les pirates nord-coréens Lazarus dans le braquage informatique de la banque centrale du Bangladesh)
  - Nombreux outils et exploits contre Windows et Windows server
    - dont EternalBlue, EternalRomance, EternalSynergy et EternalChampion
- Microsoft déclare avoir mis à disposition des correctifs pour toutes ces vulnérabilités
  - Certaines depuis plusieurs années …
  - … d'autres un mois avant la révélation de l'archive
- Les pirates du monde entier ont maintenant à leur disposition des armes informatiques puissantes
  - … et s'empressent de les utiliser !

WannaCry


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37


Petya
PetrWrap
Wannacry
2016
Shadow Brokers Leak 1
2017
Shadow Brokers Leak 2

WannaCry

- 12 mai 2017 : Première apparition de WannaCry
- Propagation utilisant l'exploit EternalBlue des outils divulgués par les Shadow brokers
  - Tous les Windows et Windows Server n'ayant pas appliqué le correctif de sécurité Microsoft MS17-010 de avril 2017 peuvent être impactés
  - Les versions plus supportées par Microsoft (XP, Server 2003) n'avaient pas de correctif
- WannaCry est très virulent
  - Propagation locale
  - Propagation sur Internet
- Propagation très rapide
  - Environ 230 000 postes/serveurs dans 150 pays la première journée

WannaCry

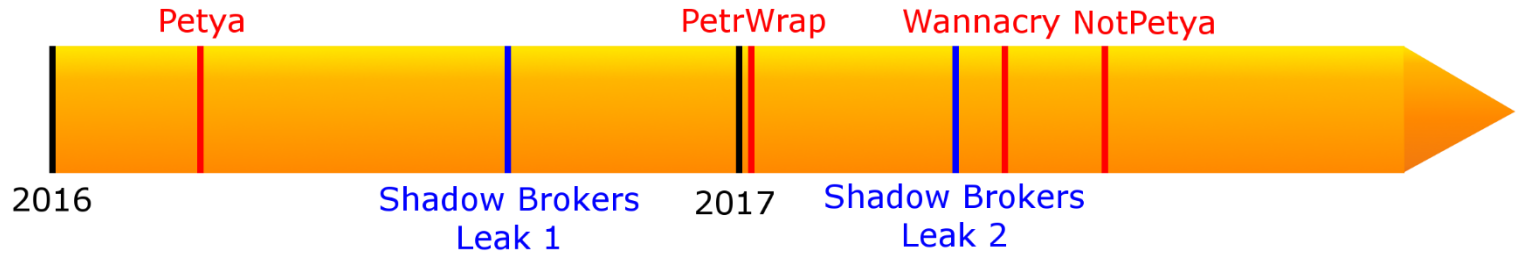
- Entre 300 000 et 400 000 victimes dans 174 pays
  - NHS (hôpitaux anglais), Telefonica, FedEx, Renault (?) …
- 97% des infections sur Windows 7
- 13 mai 2017 : Activation (fortuite) du killswitch par MalwareTech
  - Le killswitch devait complexifier l'étude du rançongiciel par ingénierie inverse dans un bac à sable
    - Un réponse à une URL aléatoire bloque l'exécution du rançongiciel
  - Celui de WannaCry est mal implémenté et interroge une URL fixe
    - En enregistrant le domaine, MalwareTech a activé le killswitch
- La propagation est ralentie

WannaCry, un flop ?

- Les conséquences de WannaCry ne sont finalement pas aussi importantes qu'on aurait pu le croire
- Propagation finalement faible
  - Dizaine d'entreprises en France (grosses PME ou filiales de groupes indépendants)
- Pas de particuliers impactés
  - Uniquement sur le port TCP/445, coupé par défaut chez les opérateurs dans le sens internet -> client
- Propagation inefficace sur Windows XP (contrairement aux attentes)
- Le killswitch a fortement ralenti la propagation
- Réaction rapide grâce à une forte médiatisation
  - Application rapide des correctifs de sécurité
- Peu rentable pour le(s) pirate(s) : environ 115 000 euros
- WannaKiwi (3 Français : B. Delpy, M. Suiche, A. Guinet)
  - Récupération de la clé de chiffrement en mémoire sous certaines conditions

NotPetya

```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   qVbndB-p6WYsk-RJZJ5Q-SQ4nAQ-S8omQy-M3zJLd-MHXhAc-QPhDXU-vQpSX4-Z3Rfgw

If you already purchased your key, please enter it below.
Key: _
```



NotPetya, un wiper

- NotPetya est un « Wiper » et non un « Ransomware »
  - L'identifiant de la victime est généré aléatoirement
  - La clé de chiffrement unique à chaque victime est définitivement supprimée à la fin de l'opération
  - L'objectif de NotPetya est donc la destruction
- 4 juillet 2017 : les pirates à l'origine de NotPetya proposent une rançon pour rendre publique la clé privée qui sert au chiffrement des fichiers
  - Uniquement des fichiers (chiffrés à haut niveau par le code empruntés à Mischa)
  - …et non de la MFT et de la MBR (donc la clé est définitivement perdue)
- Camouflage des wipers en rançongiciel
  - Pratique courante depuis quelques temps (ex : Shamoon et KillDisk)
  - Pour brouiller les pistes et les réelles motivations
- Nouvelle attaque des Russes à l'encontre des Ukrainiens ?
  - En France, une seule grosse victime : Saint-Gobain

NotPetya vs. WannaCry

- NotPetya semble plus virulent que WannaCry…
  - Plusieurs mécanismes de propagation dont le vol d'identifiants
    - Appliquer le correctif de sécurité MS17-010 n'est pas suffisant
  - Pas de killswitch
    - Et l'application du « vaccin » est une rustine peu réaliste dans des environnements complexes
- … et plus dangereux
  - Chiffrement à haut niveau (Mischa) et/ou bas niveau (Petya) selon les privilèges
- NotPetya a pourtant fait moins de dégâts
  - Attaque plus ciblée à l'encontre des entreprises
  - Propagation limitée aux réseaux locaux
  - Les extensions visées par le chiffrement ciblent plus les fichiers « professionnels » (ex : .vbs, .ova, .vbox)
- WannaCry avait forcé les entreprises à appliquer le MS17-010
  - Les conséquences auraient peut-être été tout autre si NotPetya était apparu avant WannaCry…

Bilan

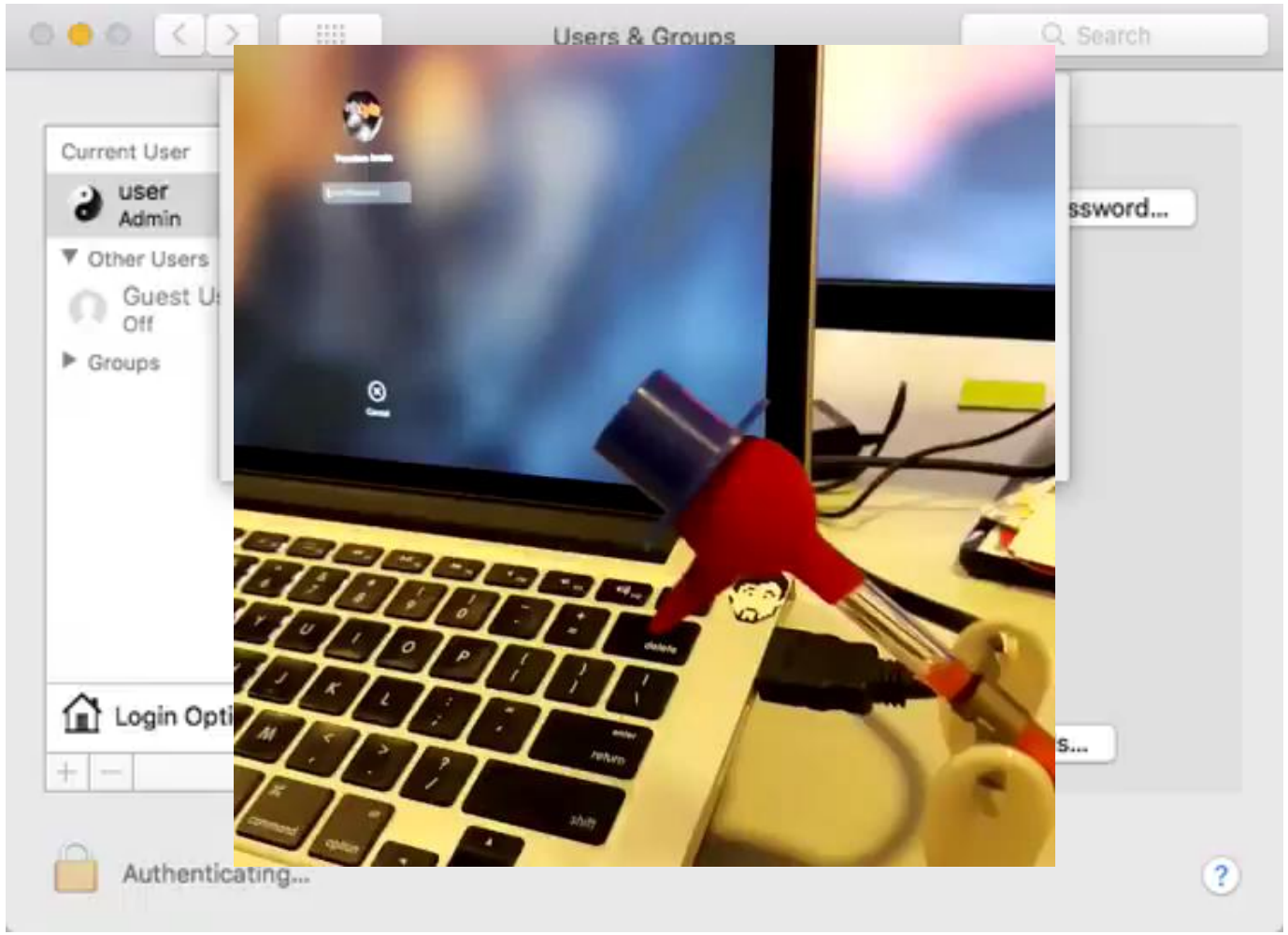
+	-
Sensibilisation du grand public	Pertes financières parfois importantes
Prise de conscience de certains dirigeants des risques numériques - Augmentation des ressources nécessaires à la SSI	Enrichissement de groupes de pirates - Financier - Technique
Preuve des capacités insoupçonnées des opérationnels	Climat de méfiance entre les Etats
Entrainement à la gestion de crise	
Développement d'outils de contremesure	

Club de la sécurité de l'information français

CLUSIF

Supply chain :
L'attaque qui vient de vos fournisseurs

#PANOCRIM



Common Criteria

FIPS Level 3 Validated 140-2

Information Security Management System ISO 27018 Certified

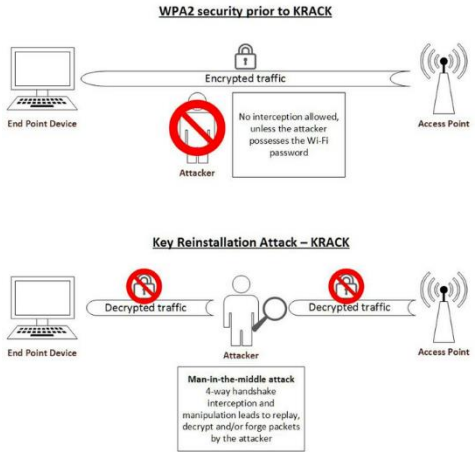
Information Security Management System ISO 27001 Certified

Des énormes "bourdes" d'éditeurs de confiance

keeper

Windows Defender

Mais aussi des problèmes de fond plus grave !

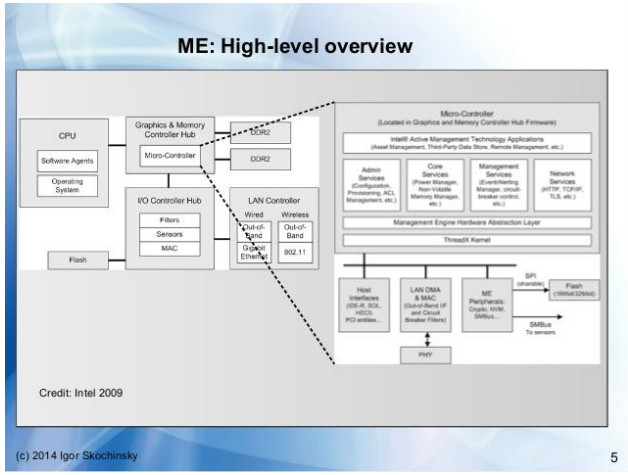


"KRACK" (Key Reinstallation Attack).

- Permet d'insérer une nouvelle clé de sécurité dans les connexions wifi
- Présent dans les implémentations de WPA2

Intel Management Engine : AMT et la suite

- Intervention à très bas niveau, rend l'attaque invisible de l'OS
- Multiples vulnérabilités très difficiles à corriger : dépend du matériel



Une incursion en 2018… Meltdown & Spectre

Plusieurs milliards de processeurs concernés

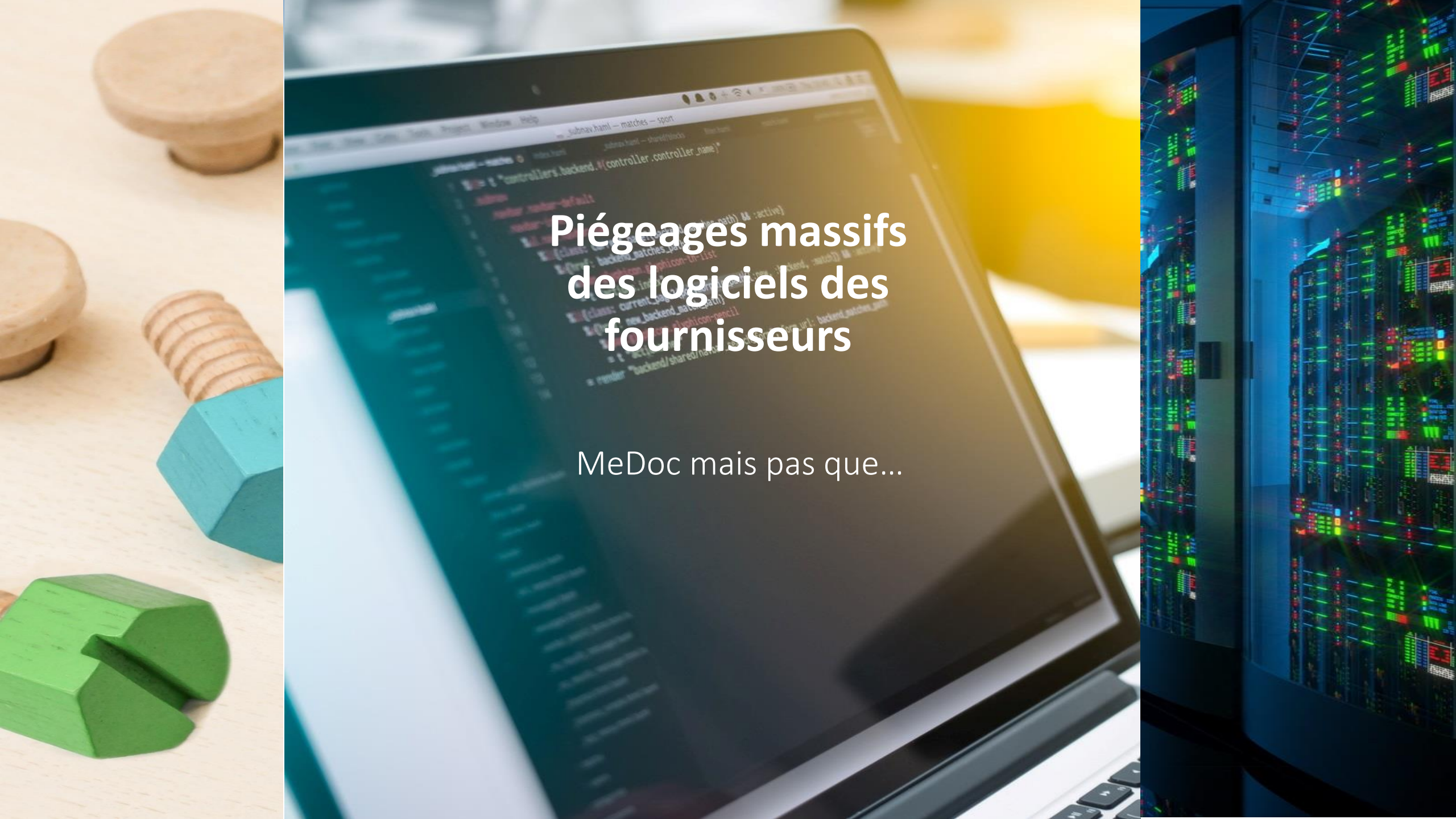
Une faille sans précédent qui permet (heureusement) uniquement d'accéder à des informations en mémoire

Imaginée dès 2005, découverte quasi simultanément par plusieurs équipes !

Et des réactions rapides qui ne sont pas toujours fiables…

Ni sans impact

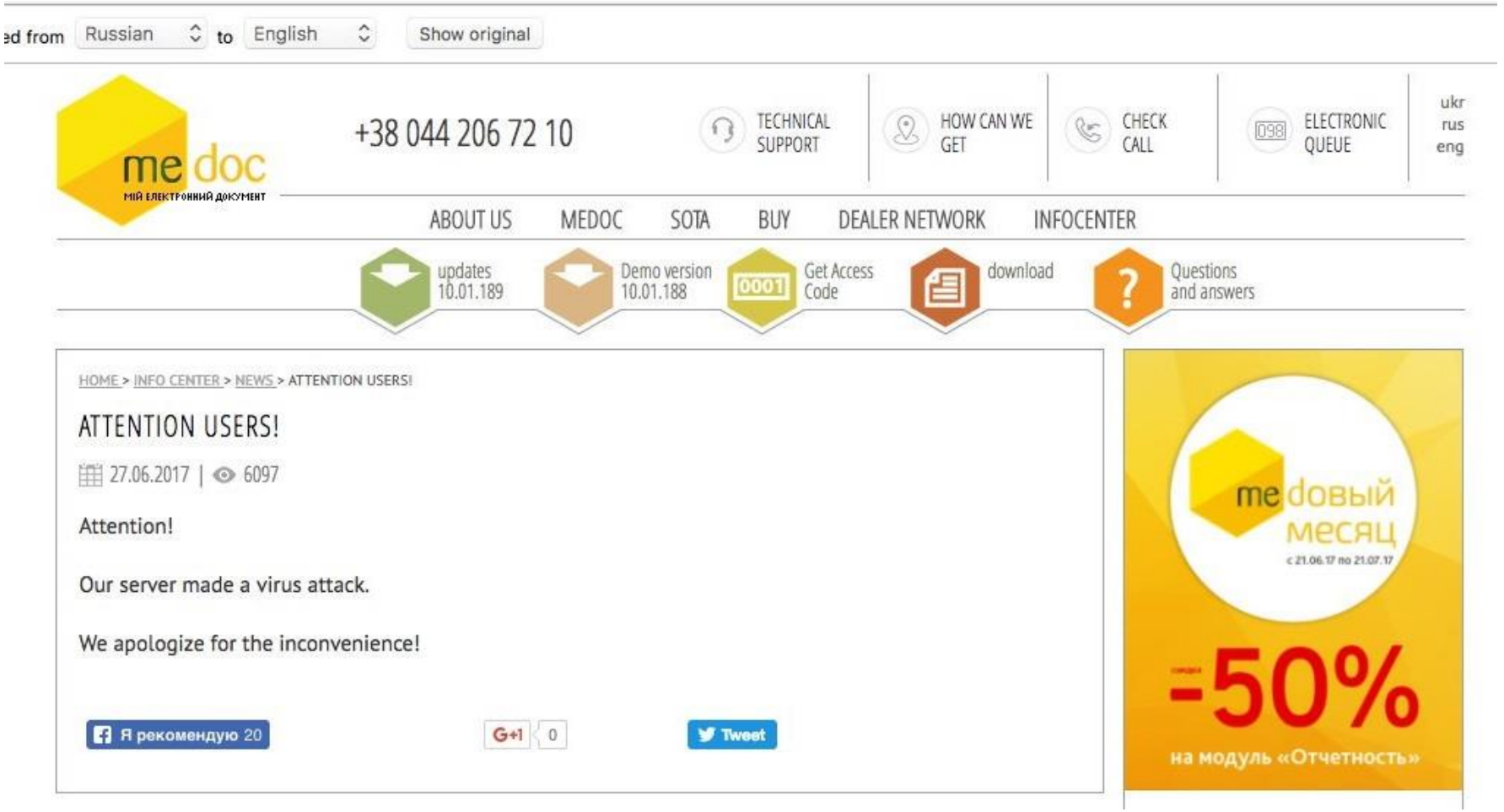
… un enfer pour les équipes de production



Piégeages massifs des logiciels des fournisseurs

MeDoc mais pas que…

NotPetya et MeDoc

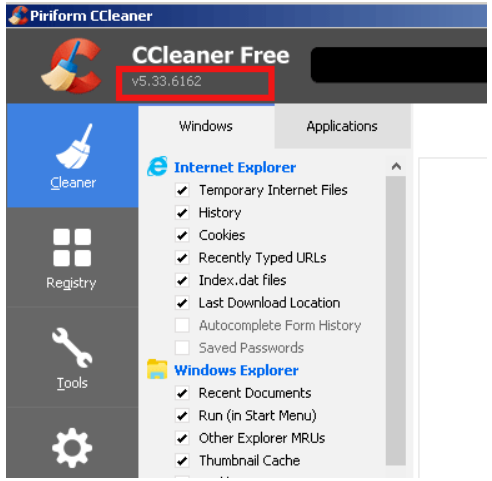


CCleaner

2 270 000 ordinateurs touchés

18 grands groupes ciblés

8 grands groupes infiltrés




```
$DomainList = array(
"singtel.corp.root",
"htcgroup.corp",
"samsung-breda",
"Samsung",
"SAMSUNG.SEPM",
"samsung.sk",
"jp.sony.com",
"am.sony.com",
"gg.gauselmann.com",
"vmware.com",
"ger.corp.intel.com",
"amr.corp.intel.com",
"ntdev.corp.microsoft.com",
"cisco.com",

"uk.pri.o2.com",
"vf-es.internal.vodafone.com",

"linksys",
"apo.epson.net",
"msi.com.tw",
"infoview2u.dvrdns.org",
"dfw01.corp.akamai.com",
"hq.gmail.com",
"dlink.com",

"test.com");
```

Piégeages ciblés des infrastructures utilisées

Une menace moins visible mais bien présente

Zoom sur une attaque ciblant les infogérants

CloudHopper

15 pays ciblés

+70 variantes de backdoor et de trojans utilisées

Vecteur d'intrusion par spear-phishing

Début de la campagne en 2014

Les infrastructures réseau compromis des infogérants ont été utilisées comme routes d'exfiltration de données

Une problématique commune : l'effet de masse

Des milliers
de PCs et serveurs pour Cloud Hopper

Des centaines de milliers
de machines pour NotPetya

2,25M
d'utilisateurs CCLEANER

Des millions
d'équipements pour KRACK

Des milliards
de processeurs pour
Spectre/Meltdown

Un risque systémique à anticiper

L'utilisation d'outils autorisés dans l'entreprise par des attaquants pour se **déployer ou se déplacer** est un challenge qui va grandir.

L'observation des **comportements des ressources autorisées** sera un challenge pour 2018 et le futur.

La capacité **d'isolation rapide** et de détermination rapide du risque sera un facteur clé pour limiter les pandémies.

CLUSIF

Vecteurs d'attaques innovants - CLOUD

Le cas de la NSA et l'armée US

- Des documents top-secret de l'armée américaine et de la NSA exposés sur les serveurs sur AWS S3. L'entité en question : INSCOM (United States Army Intelligence and Security Command)

- Le 27/09/2017 : Upguard découvre "un bucket" d'AWS S3 en accès public permettant à n'importe qui d'accéder au contenu du "bucket", son « repository » rattaché au sous-domaine INSCOM.

Le cas de la NSA et l'armée US

- Les serveurs exposés ont été découverts par l'équipe UpGuard. Cette équipe a pu **accéder à de nombreux documents dont 3 en "libre de téléchargement".**

- Un des fichiers fut un **.ova (Oracle Virtual Appliance)** qui était une image d'une machine virtuelle et le disque virtuel associé.

- Les chercheurs n'ont pas pu booter sur cette VM. Cependant les métadonnées stockées dans le disque virtuel rattaché ont **pu leur permettre d'identifier un certain nombre de fichiers sensibles** avec des attributs tels que « TOP SECRET and NOFORN (NO FOReign Nationals) »

- Des informations concernant un sous-traitant, Invertix, montrent les clés privées utilisées, appartenant aux administrateurs Invertix, pour accéder à des systèmes ainsi que des hashs de mots de passe, pouvant éventuellement être craqués, **qui pourraient être utilisés pour compromettre d'autres systèmes** s'ils sont toujours valides.

Encore Amazon…

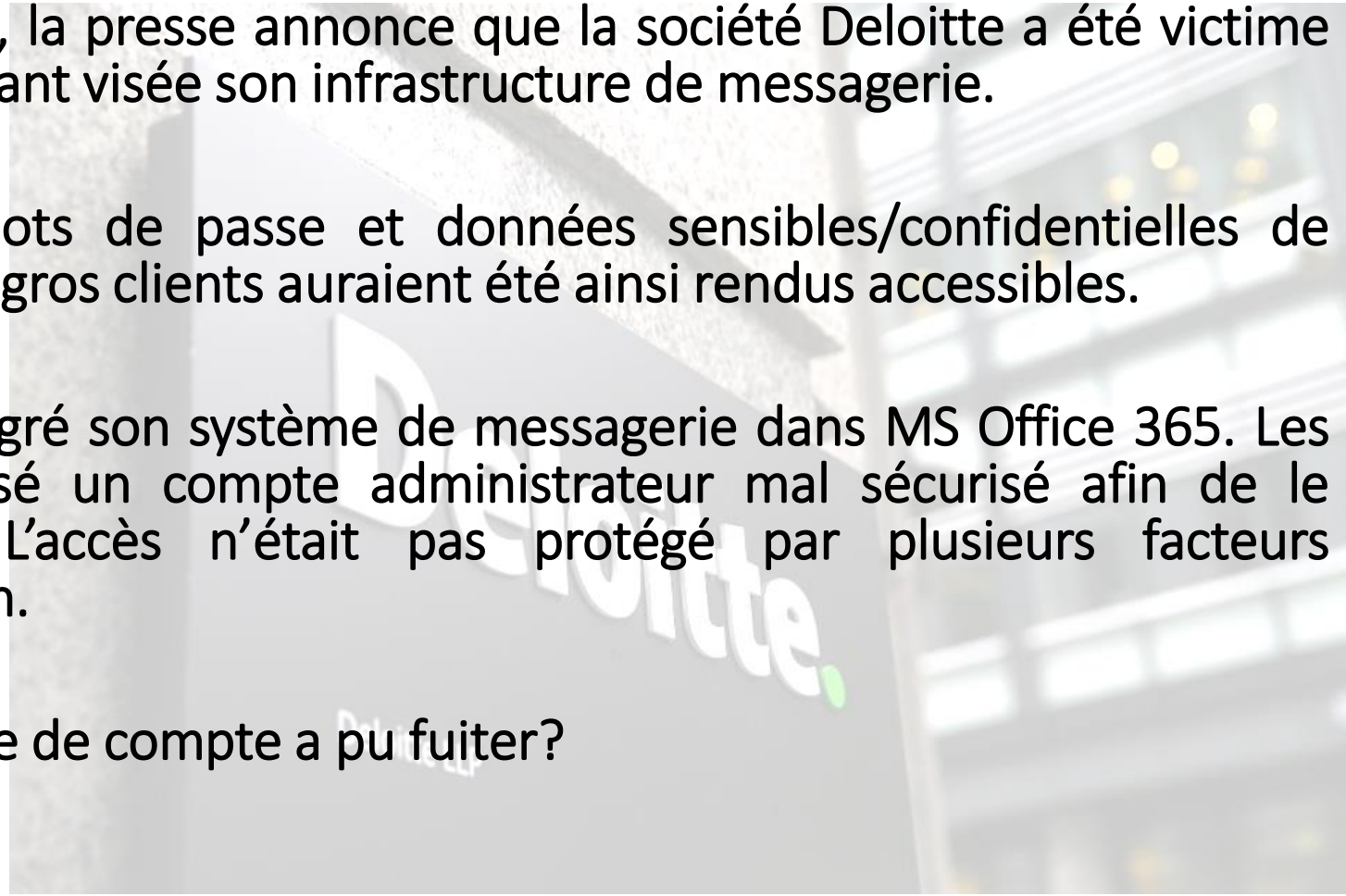
- Des données du Pentagone stockées sur AWS accessibles publiquement
  - A travers Amazon Web Services, le Pentagone a laissé pendant des mois, voire des années, l'accès public à des milliards de données collectées en ligne.
    - Source https://www.silicon.fr/donnees-pentagone-stockees-aws-190971.html?inf_by=5a43d377671db8c10a8b4a9b
- Accenture victime d'une fuite de données à la suite de l'exposition de plusieurs espaces de stockage AWS S3
    - Source https://www.cyberveille-sante.gouv.fr/cyberveille/244-accenture-potentiellement-victime-dune-fuite-de-donnees-suite-lexposition-de
- Another misconfigured Amazon S3 server leaks data of 50,000 Australian employees
    - Source https://www.scmagazine.com/contractor-misconfigures-aws-exposes-data-of-50000-australian-employees/article/704873/

Le cas de la société Uber

- Fin novembre 2017, toute la presse en parle, la société de VTC Uber a subi une attaque en 2016 et l'a gardée secrète
- Pour rappel :
  - 2 pirates ont dérobé plus de 50 millions de comptes clients et chauffeurs (incluant numéros de téléphone, adresse email et noms) et ont demandé une rançon de 100k$ à Uber pour la destruction de ces données et leur discrétion.
- Pratiques de développement en cause :
  - Accès au GitHub privé utilisé par les ingénieurs d'Uber (MITRE CWE-798 ou mot de passe enregistré en dur permettent aux attaquants de "bypasser" le processus d'authentification mis en place)
  - Utilisation des comptes récupérés sur Github pour accéder aux données stockées dans ses « buckets » sur AWS S3.
  - Par la suite, les pirates ont récupérés une archive contenant les informations sur les chauffeurs et clients.

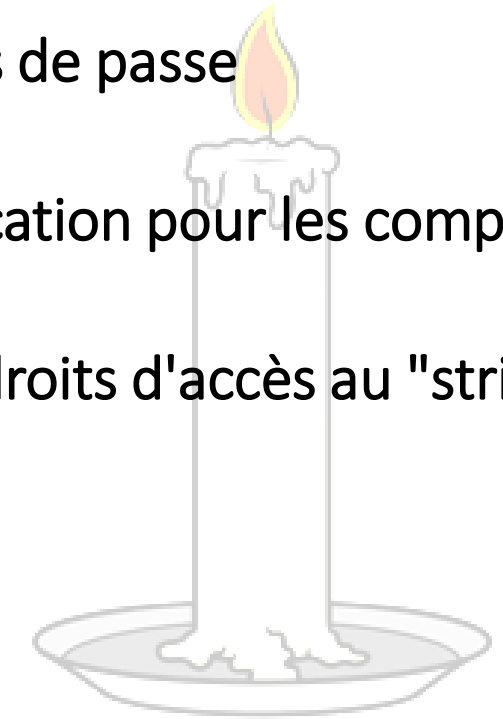
Le cas du cabinet de conseil Deloitte

- Septembre 2017, la presse annonce que la société Deloitte a été victime d'une attaque ayant visée son infrastructure de messagerie.
- Les comptes, mots de passe et données sensibles/confidentielles de certains de leurs gros clients auraient été ainsi rendus accessibles.
- Deloitte avait migré son système de messagerie dans MS Office 365. Les pirates ont utilisé un compte administrateur mal sécurisé afin de le compromettre. L'accès n'était pas protégé par plusieurs facteurs d'authentification.
- Comment ce type de compte a pu fuiter?



Qu'aurait-il fallu faire ?

- Gestion différenciée des niveaux de privilège
- Changement régulier des mots de passe
- Plusieurs facteurs d'authentification pour les comptes à privilèges élevés
- Restrictions des privilèges ou droits d'accès au "strict nécessaire"



Que retenir au final…

- Le volume de données dans le cloud ne cesse de grossir. Ce qui conduit inévitablement à une augmentation des surfaces d'attaques possibles et à des risques potentiellement plus importants.

> Contrary to what many might think, the main responsibility for protecting corporate data in the cloud lies not with the service provider but with the cloud customer. "We are in a cloud security transition period in which focus is shifting from the provider to the customer," Heiser says. "Enterprises are learning that huge amounts of time spent trying to figure out if any particular cloud service provider is 'secure' or not has virtually no payback."

Source : https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html

CLUSIF

Vecteurs d'attaques innovants - IoT

2017… dans le prolongement de 2016 !

Jouets – La vie privée en jeu

- Aucun code d'accès ou procédure d'a connectés
  - Mon amie Cayla (poupée) et I-Que
  - Ecoute de l'enfant jusqu'à 20m de c
  - Communication avec l'enfant jusqu'
- Collecte des données vocales
  - Non nécessaire au fonctionnement
  - Transmission à des tiers
  - Transmission des données dans des protection sur la vie privée
- Matraquage publicitaire
  - Les jouets prononcent régulièreme faire la publicité d'autres produits

PANORAMA DE LA CYBERCRIMINALITE -

Véhicules – Vols sans effraction

- En 2016, **75%** des vols de voitures ont été réalisés par ***mouse jacking***
- Inefficacité du principe des télécommandes à code tournant
  - **Interception et reproduction du code** pour ouvrir ou démarrer le véhicule
- Attaque par **amplification du signal radio**
  - Ouverture et démarrage du véhicule connecté sans clé
  - Alarmes et systèmes d'immobilisation désactivables
  - Réalisable jusqu'à 100m
  - Attaque simple, aucun matériel coûteux ou spécifique
  - Tests réalisés par le club automobile ADAC
  - **24 véhicules de 19 constructeurs** différents testés étaient **vulnérables**

PANORAMA DE LA CYBERCRIMINALITE - ANNEE 2016 11/01/2017

Mirai et la suite…

- Adaptation / évolution du code source MIRAI
  - Infection d'objets connectés : Caméra, box opérateur et routeurs
- Exploitation de routeurs : Brickerbot, Satori, IoT_reaper, IoTroop…
  - Failles diverses rapidement exploitées (Netgear, Linksys, Dlink, Goahead…)
  - Utilisation de « 0-day » : Satori - Huawei CVE-2017-17215
  - Sophistication des outils (ex : IoTroop)
- Un IoT botnet « bienveillant » : Hajime
  - Avril 2017
  - Efficacité modérée (non persistance…)
  - Déontologie discutable….

> Just a white hat, securing some systems.
>
> Important messages will be signed like this!
>
> Hajime Author.
>
> Contact CLOSED
>
> Stay sharp!

Des objets connectés qui nous écoutent ?

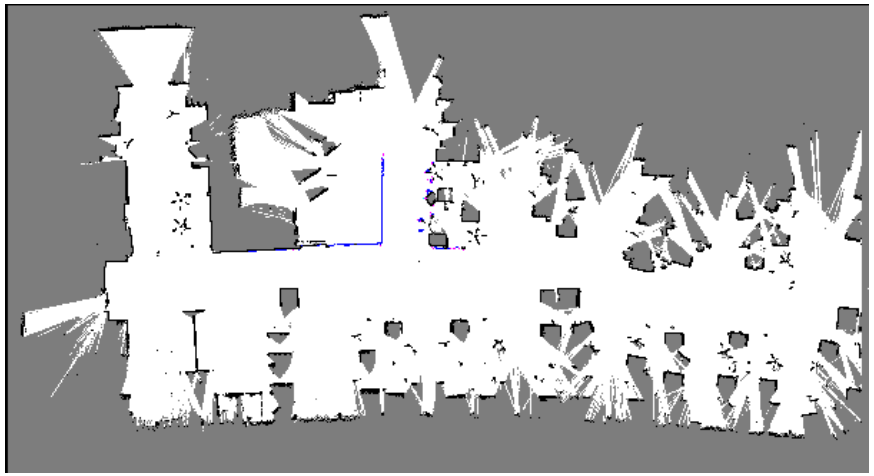
- Des objets connectés de plus en plus présents
  - Assistants personnels, jouets, objets du quotidien (TV, aspirateurs, clim…)

- Mars 2017 : How the CIA Can Hack Your Phone, PC, and TV (Says WikiLeaks)
- Août 2017 : This hack lets Amazon Echo 'remotely snoop' on users
- Novembre 2017 : Bluetooth hack affects 20 Million Amazon Echo & Google Home Devices
- Novembre 2017 : les raters, « tacherons du big data » qui nous écoutent pour notre bien - validation de la qualité de la réponse au service

- 4 décembre 2017 : mise en demeure publique pour atteinte grave à la vie privée en raison d'un défaut de sécurité (CNIL)
  - La CNIL contre GENESIS INDUSTRIES LIMITED
    - poupée « My Friend Cayla » et robot « I-QUE »
    - Destruction des jouets en Allemagne – février 2017

Des objets connectés qui nous écoutent ?

- Des objets connectés de plus en plus présents
  - Aspirateurs autonomes
- Déclaration de Colin Angle en juillet 2017 (iRobot Corp / Roomba)
  - "There's an entire ecosystem of things and services that the smart home can deliver once you have a rich map of the home that the user has allowed to be shared,"
- Présentation au 34C3…
  - Un objet très intéressant : Gyroscope, accéléromètre capteur de distance laser (LIDAR) sous Linux Ubuntu (Xiaomi vacuum cleaning robot)



et du coté de Solihull, le 24/9/2017…

CLUSIF

Bitcoin: sky is the limit …or is it the hack?

Breaking news: Explosion du cours du bitcoin !

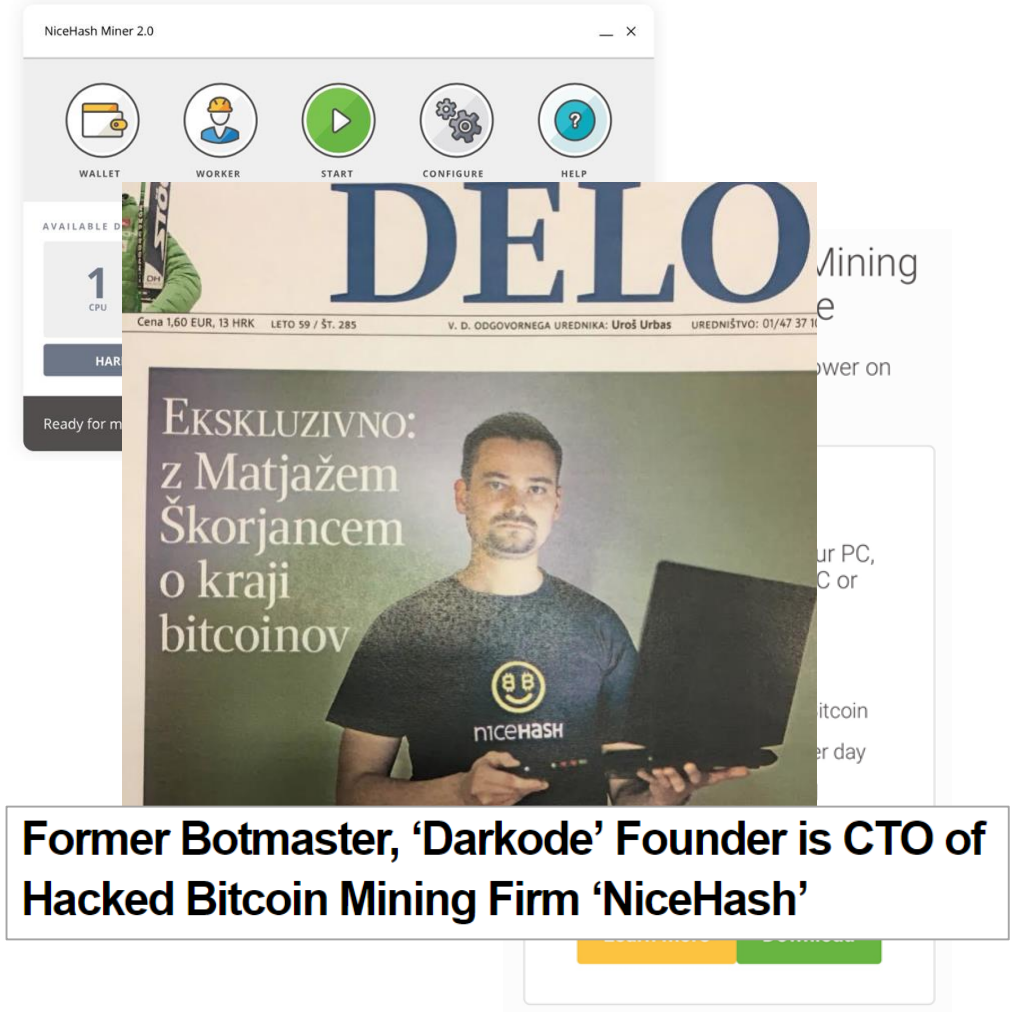
Mais aussi une explosion de l'intérêt des cybercriminels…

Minage

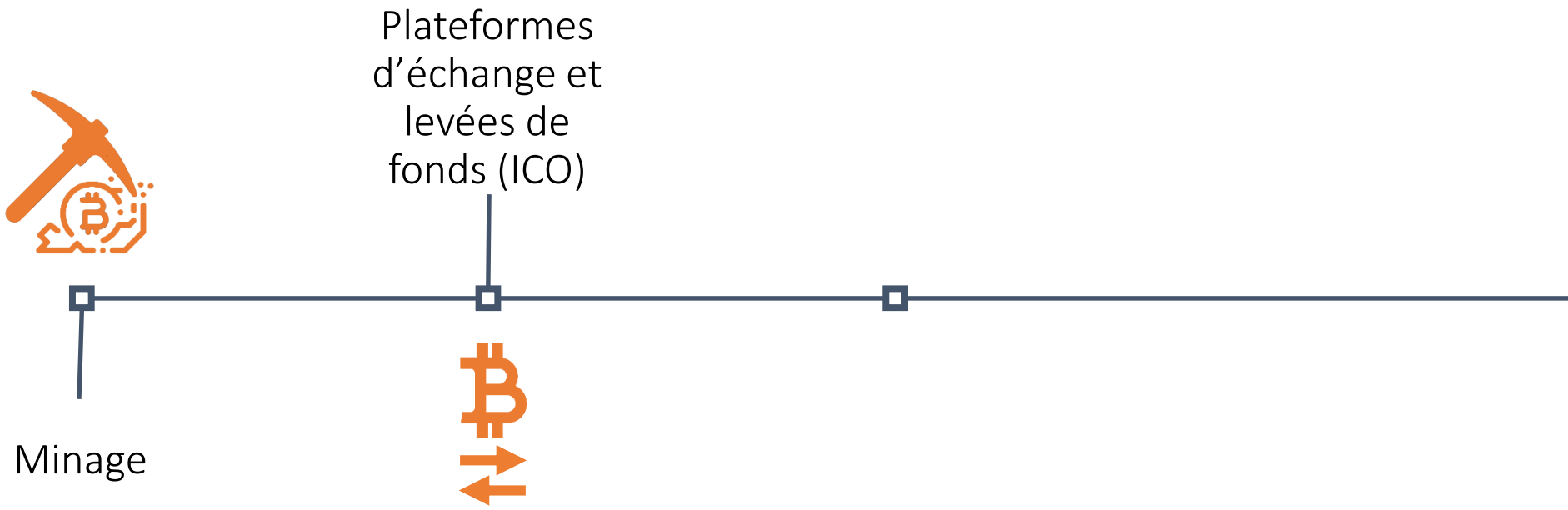
Des attaques qui visent les « mineurs »

NiceHash est une place de marché mettant en relation des personnes ayant des capacités de calcul à louer.

Décembre 2017 : la société est victime d'une intrusion « avancée » sur ses serveurs et 4 700 BTC sont ainsi détournés, i.e. près de 64 millions de dollars.



Mais aussi une explosion de l'intérêt des cybercriminels…



Des attaques qui visent les « Exchanges » / ICOs

Du plus avancé…

Rejeu d'une preuve de transaction valide grâce à un bug (de 1 caractère) dans le code source. **600 000$.**

Faille dans le code du smart contrat Ethereum malgré plusieurs revues de code par de nombreux spécialistes du domaine. **30M$**.

Des attaques qui visent les « Exchanges » / ICOs

… au plus simple

COINDASH

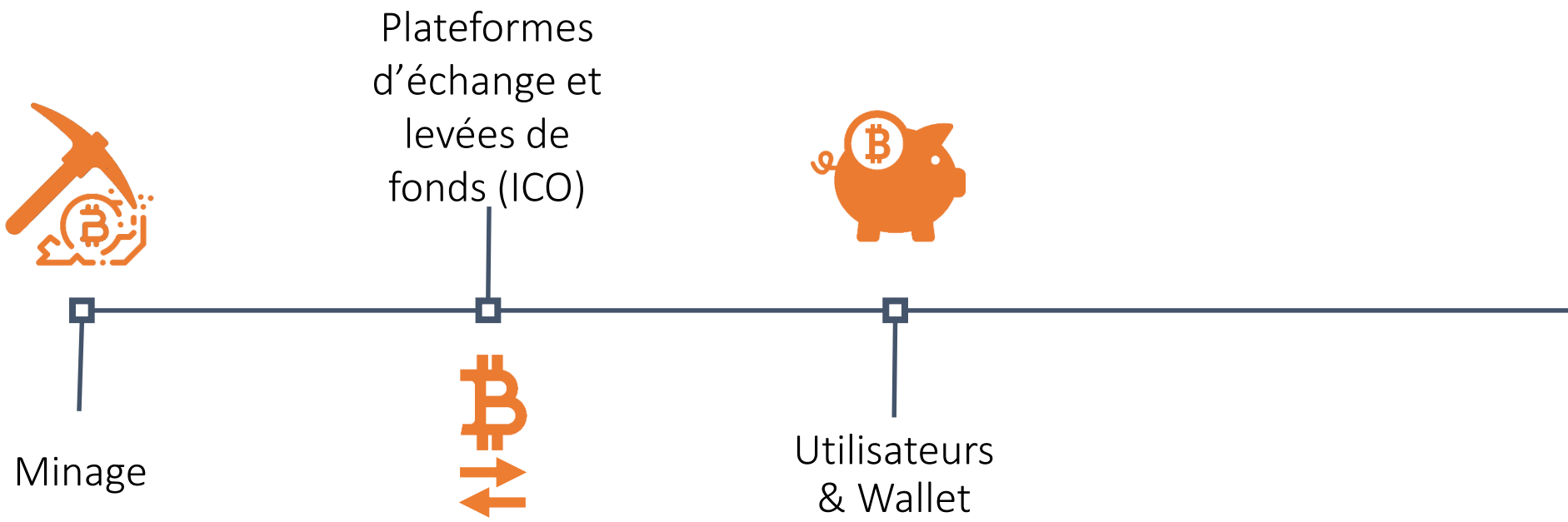
Un attaquant a pris le contrôle du site web et a modifié aléatoirement l'adresse du paiement pour la levée de fond. **7 millions de $ détournés** pour 6,4m collectés…

enigma

Le mot de passe du CEO, compromis lors de fuites précédentes sur Internet, était utilisé pour son email, le compte Slack, la mailing list et le site web. **500 000$.**

Une technologie certes solide mais son environnement pas toujours…

Mais aussi une explosion de l'intérêt des cybercriminels…



Des codes malfaisants qui visent nos portefeuilles

Cryptocurrency stealer

“Nearly 150 Breeds Of Bitcoin-Stealing Malware In The Wild, Researchers Say”, 2014, Forbes

“Quant Trojan upgrade targets Bitcoin, cryptocurrency wallets”, 2017, ZDNet

“Hackers Infiltrate Official Bitcoin Gold Wallet Repository”, 2017, CCN

+ astucieux

CRYPTOSHUFFLER

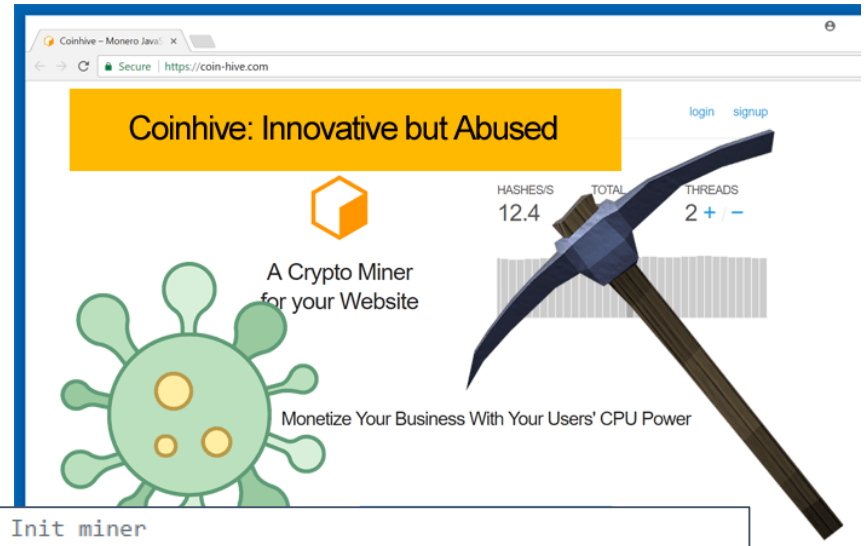
Le cheval de Troie change l’adresse de destination d’un paiement dans le presse-papier de l’utilisateur. **160 000$.**

La "vraie" nouveauté de 2017 : devenir mineur à son insu !

CoinHive est un outil Javascript de minage de la crypto-monnaie **Monero.**

Facilement intégrable à un site web, l'outil se pose comme une alternative à la publicité (ex: ThePirateBay).

« Drive By Mining » : Nouvelle source de revenu facile à exploiter pour les cybercriminels (piégeage de site web ou logiciel malfaisant dédié)…




```
// Init miner
function init({ siteKey, interval = 1000, threads = null,
  // Create miner
  if (!username) {
    miner = new CoinHive.Anonymous(siteKey);
  } else {
    miner = new CoinHive.User(siteKey, username);
  }
```

Panorama 2017 – synthèse pour Aristote

- Attaques destructives
- Attaques via des tierces parties
- Vecteurs d'attaques innovants : le Cloud et l'IoT
- Bitcoin & Co : l'envol des prix attire les cybercriminels

- En janvier, on a également abordé :
  - La gestion de crise et ses limites
  - Elections et cyber, les enjeux géopolitiques
  - Rançon : payer ou ne pas payer ?
  - Ils ont été arrêtés : le Darknet mais pas que…
  - Les sujets émergents