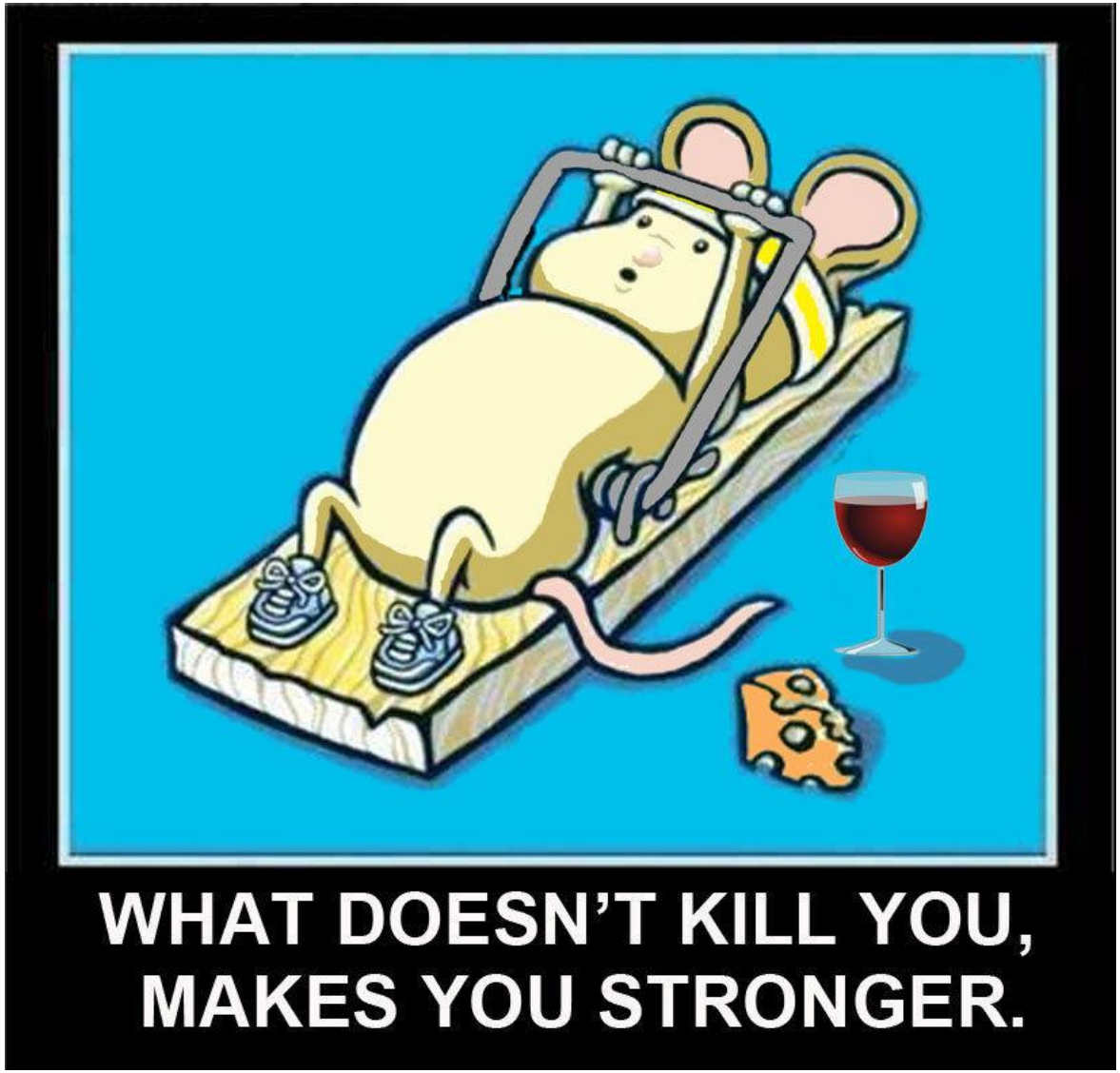
Le Chat et la Souris 2

Pascal Le Digol
Country Manager France

Le Jeu du Chat et de la Souris…

50 ans d'histoire de l'informatique

Regardons sur une période plus courte…



La souris ne touche pas tout le monde ?

Apple » Mac Os X : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

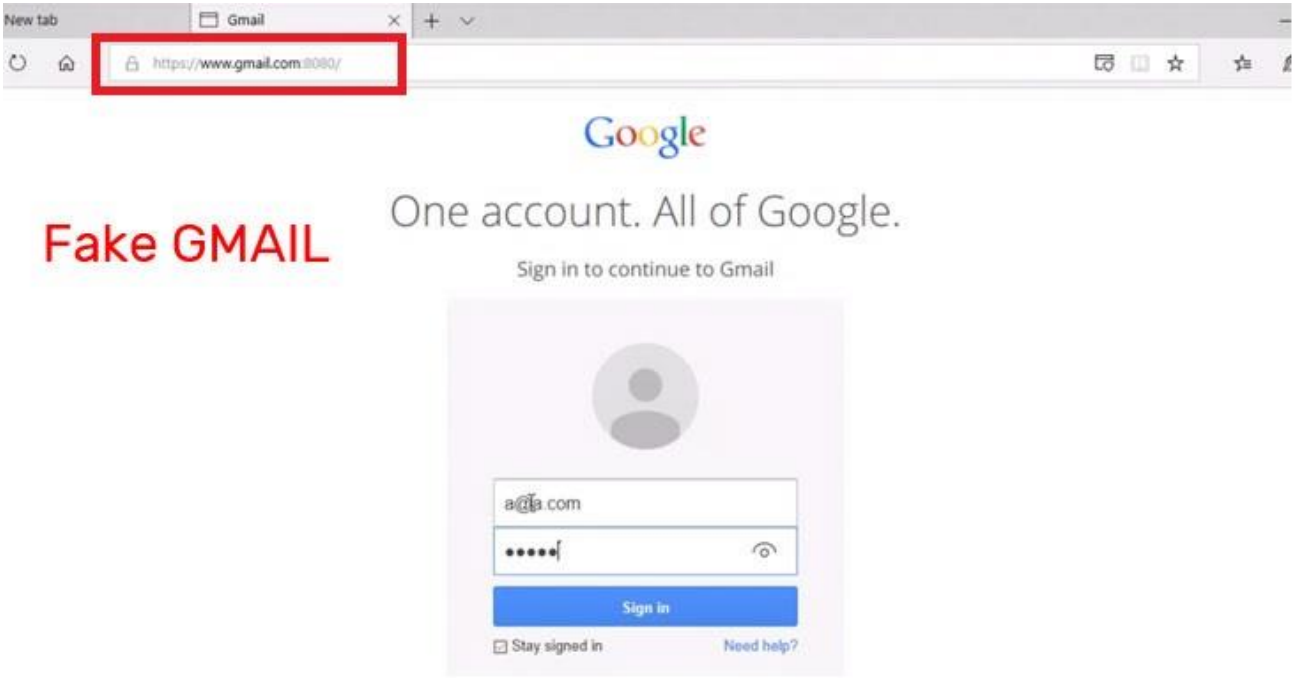
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-8897	264			2018-05-08	2019-01-03	7.2	None	Local	Low	Not required	Complete	Complete	Complete
A statement in the System Programming Guide of the Intel 64 and IA-32 Architectures Software Developer's Manual (SDM) was mishandled in the development of some or all operating-system kernels, resulting in unexpected behavior for #DB exceptions that are deferred by MOV SS or POP SS, as demonstrated by (for example) privilege escalation in Windows, macOS, some Xen configurations, or FreeBSD, or a Linux kernel crash. The MOV to SS and POP SS instructions inhibit interrupts (including NMIs), data breakpoints, and single step trap exceptions until the instruction boundary following the next instruction (SDM Vol. 3A; section 6.8.3). (The inhibited data breakpoints are those on memory accessed by the MOV to SS or POP to SS instruction itself.) Note that debug exceptions are not inhibited by the interrupt enable (EFLAGS.IF) system flag (SDM Vol. 3A; section 2.3). If the instruction following the MOV to SS or POP to SS instruction is an instruction like SYSCALL, SYSENTER, INT 3, etc. that transfers control to the operating system at CPL < 3, the debug exception is delivered after the transfer to CPL < 3 is complete. OS kernels may not expect this order of events and may therefore experience unexpected behavior when it occurs.													
2	CVE-2018-5383	310			2018-08-07	2018-10-18	4.3	None	Local Network	Medium	Not required	Partial	Partial	None
Bluetooth firmware or operating system software drivers in macOS versions before 10.13, High Sierra and iOS versions before 11.4, and Android versions before the 2018-06-05 patch may not sufficiently validate elliptic curve parameters used to generate public keys during a Diffie-Hellman key exchange, which may allow a remote attacker to obtain the encryption key used by the device.														
3	CVE-2018-4253	125		DoS Bypass	2018-06-08	2018-07-13	7.1	None	Remote	Medium	Not required	Complete	None	None
An issue was discovered in certain Apple products. macOS before 10.13.5 is affected. The issue involves the "AMD" component. It allows local users to bypass intended memory-read restrictions or cause a denial of service (out-of-bounds read of kernel memory) via a crafted app.														
4	CVE-2018-4251	284			2018-06-08	2018-07-13	7.1	None	Remote	Medium	Not required	None	Complete	None
An issue was discovered in certain Apple products. macOS before 10.13.5 is affected. The issue involves the "Firmware" component. It allows attackers to modify the EFI flash-memory region that a crafted app that has root access.														
5	CVE-2018-4249	190		DoS Exec Code Overflow	2018-06-08	2018-07-17	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
An issue was discovered in certain Apple products. iOS before 11.4 is affected. macOS before 10.13.5 is affected. tvOS before 11.4 is affected. watchOS before 4.3.1 is affected. The issue involves pktmnglr_ipfilter_input in com.apple.packet-mangler in the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (integer overflow and stack-based buffer overflow) via a crafted app.														
6	CVE-2018-4243	119		Exec Code Overflow	2018-06-08	2018-07-17	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
An issue was discovered in certain Apple products. iOS before 11.4 is affected. macOS before 10.13.5 is affected. tvOS before 11.4 is affected. watchOS before 4.3.1 is affected. The issue involves the "Kernel" component. A buffer overflow in getvolattrlist allows attackers to execute arbitrary code in a privileged context via a crafted app.														
7	CVE-2018-4242	119		DoS Exec Code Overflow Mem. Corr.	2018-06-08	2018-10-31	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
An issue was discovered in certain Apple products. macOS before 10.13.5 is affected. The issue involves the "Hypervisor" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.														

https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-156/Apple-Mac-Os-X.html

Faille du navigateur Safari

- Permet d'afficher l'URL d'un site Web sûr, alors que les utilisateurs sont redirigés vers un autre site Web



(*faille patchée le 17 Septembre 2018 par Apple*)

En vrac…

Critical MacOS Mojave
vulnerability bypasses system

Un malware s'attaque à Mac OS

Sécurité : Le logiciel malveillant se fait passer pour un logiciel de sécurité afin de pousser les utilisateurs Mac

Clubic Tech › Logiciel › Sécurité informatique › Virus et failles logiciel › Malware

ZDNet

Par

L'éditeur Intego
l'existence d'un
d'Apple.

Déguisé en faux
(search engine
d'images de Goo

Un malware qui

Apple : le nombre de malwares sur Mac a presque triplé en 2017

Par Paolo GAROSCIO
Le 13 mars 2018

0

La belle époque où « *les Macs n'avaient pas de virus* » semble bel et bien révolue. Même si, en réalité, des virus et autres malwares ciblant les ordinateurs d'Apple ont toujours existé, ces derniers étaient effectivement bien moins nombreux que ceux ciblant Windows. C'est encore le cas... mais la menace contre les Macs se fait de plus en plus virulente.

Même nos célébrités l'ont compris… à force…

PIPPA HACK Pippa Middleton iCloud photo hack – how did it happen and how to keep your pictures safe

We reveal the simple tips for keeping iCloud data private

by holly christodoulou

26th September 2016, 3:53 pm | Updated: 27th September 2016, 2:52 am

COMMENT NOW

PIPPA Middleton's iCloud account was hacked for 3,000 private photographs - including some snaps of Prince George and Princess Charlotte.

Nathan Wyatt, 25, has been released on bail after he was quizzed by cops over the weekend.

ence and Other Celebs
de Photos Circulate on the

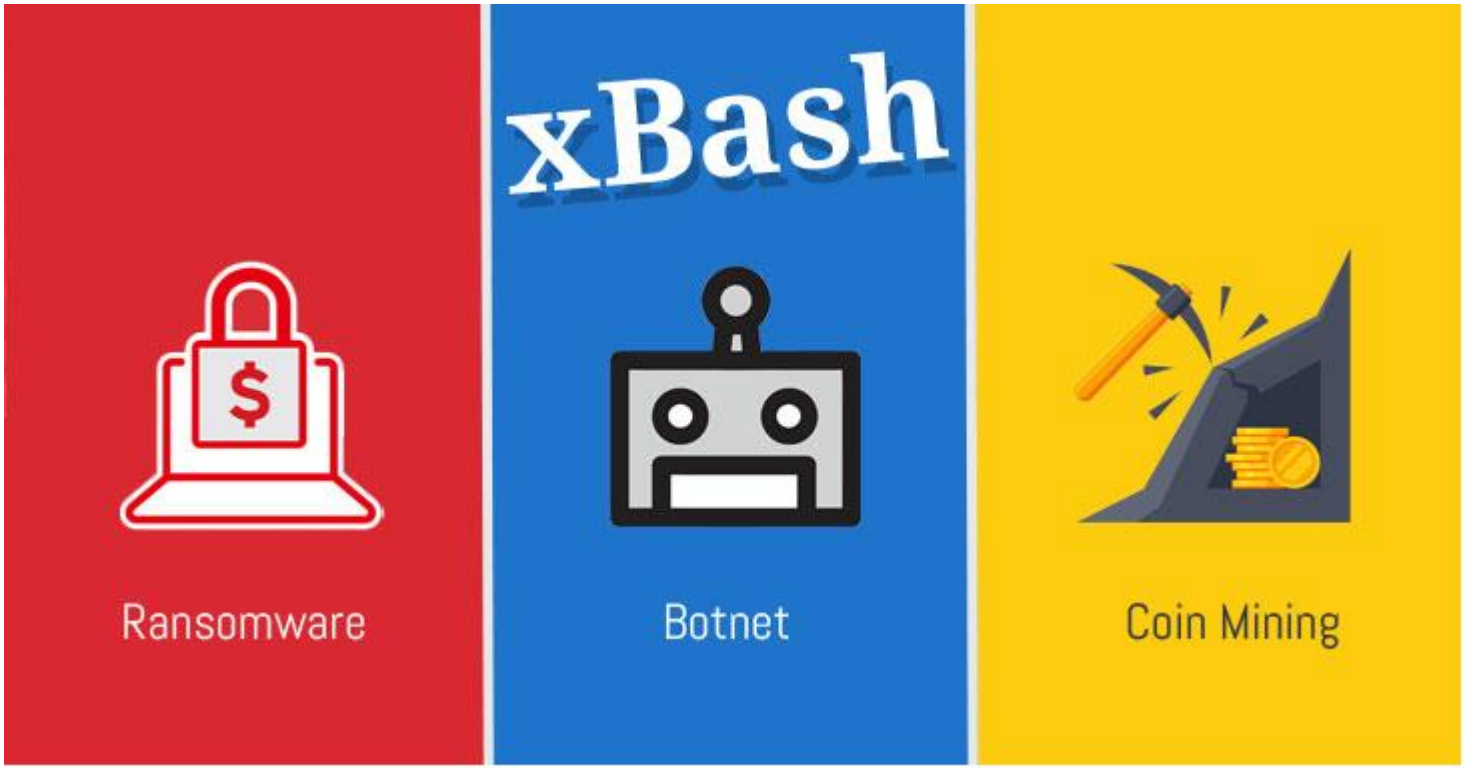
il y aura toujours quelqu'un qui profite d'une « opportunité »

Payant, anonyme, sans partage des fichiers avec la communauté Antivirus contrairement à VirusTotal

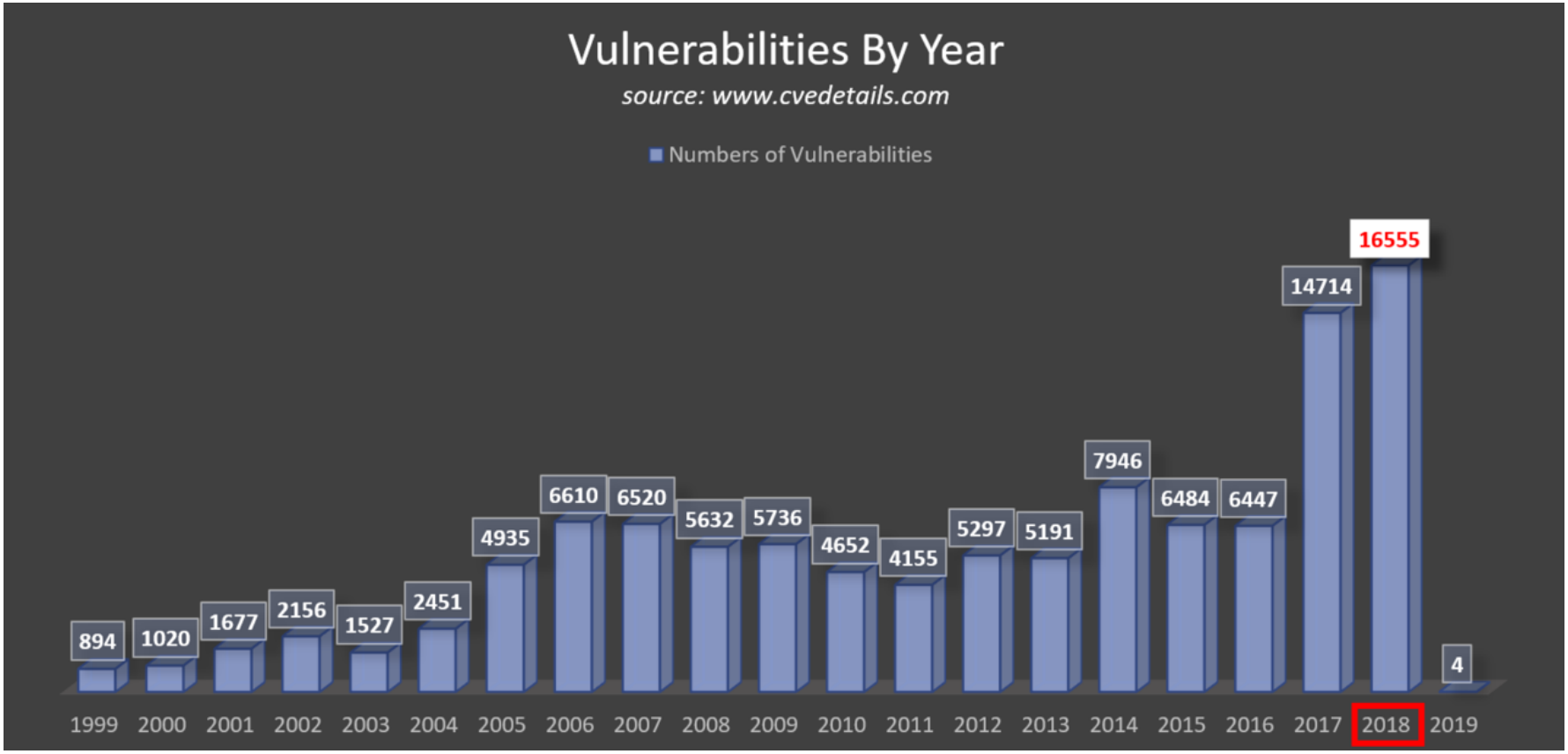
Extradé aux US , 14 ans de prison …

Hacking As A Service

Pourquoi choisir une attaque plutôt qu'une autre…



Comme s'il n'y avait pas assez de l'ingéniosité des pirates …



D’ailleurs…

DragonBlood

Cracking WPA3 Wi-Fi Password

Vulnérabilités dans les chipsets

Software Engineering Institute | Carnegie Mellon University

Broadcom : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6
Sort Results By : CVE Number Descending CVE Nur
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vu
1	CVE-2017-11122	200		+I
	On Broadcom BCM4355C0 Wi-Fi chips 9.44.78.27.			
2	CVE-2017-11121	119		Do
	On Broadcom BCM4355C0 Wi-Fi chips 9.44.78.27. leading to denial of service or other effects, aka E			
3	CVE-2017-11120	119		Ov
	On Broadcom BCM4355C0 Wi-Fi chips 9.44.78.27. B-V2017061204.			
4	CVE-2017-9417	284		Ex
	Broadcom BCM43xx Wi-Fi chips allow remote atta			
5	CVE-2017-6957	119		Ex
	Stack-based buffer overflow in the firmware in Br execute arbitrary code via a crafted reassociation			
6	CVE-2017-6956	119		Ex
	On the Broadcom Wi-Fi HardMAC SoC with fbt firn sends a long R0KH-ID field in a Fast BSS Transitio			
7	CVE-2014-2046	310		+I
	cgi-bin/rpcBridge in the web interface 1.1 on Broa request to the config.getValuesHashExcludePaths			
8	CVE-2012-2619	20		Do
	The Broadcom BCM4325 and BCM4329 Wi-Fi chip a denial of service (out-of-bounds read and Wi-Fi			

La mise à jour iOS 10.3.3 livrée le 19 juillet par Apple corrige la vulnérabilité Broadpwn qui affecte les puces WiFi de Broadcom utilisées dans les matériels iOS. Il y a 15 jours, Google avait déjà livré un patch pour les matériels Android pour corriger cette même vulnérabilité.

Impact

An unauthenticated, remote attacker may be able to create a denial-of-service condition.

Spectre / Meltdown

	Meltdown	Spectre
Touchés	Intel	Intel, AMD, ARM
Entrée	Accès permettant d' exécuter du code	Accès permettant d' exécuter du code
Méthode	Elévation de privilèges + exécution d'instructions étrangères.	Exécution d'instructions étrangères
Danger	Rupture de l'isolation entre l'applicatif et le système d'exploitation.	Rupture de l'isolation entre différentes applications.
Impact	Accès au contenu de la mémoire depuis l'espace utilisateur.	Accès au contenu de la mémoire d'un autre processus.
Contre-mesure	Correctifs à venir, mais dégradation des performances	Inexistante (au mieux, des correctifs applicatifs au cas par cas)

3 Janvier 2018

Source : @MaliciaRogue

Sauvés par le RGPD ?

« Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque »

Article 32

Source: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

Article 32 plus que nécessaire

EXPERTISES

PROTECTION DES DONNÉES

Les entreprises françaises plus confrontées à la perte de données qu'ailleurs dans le monde

le 22-03-2019
Par Dirk Basyn

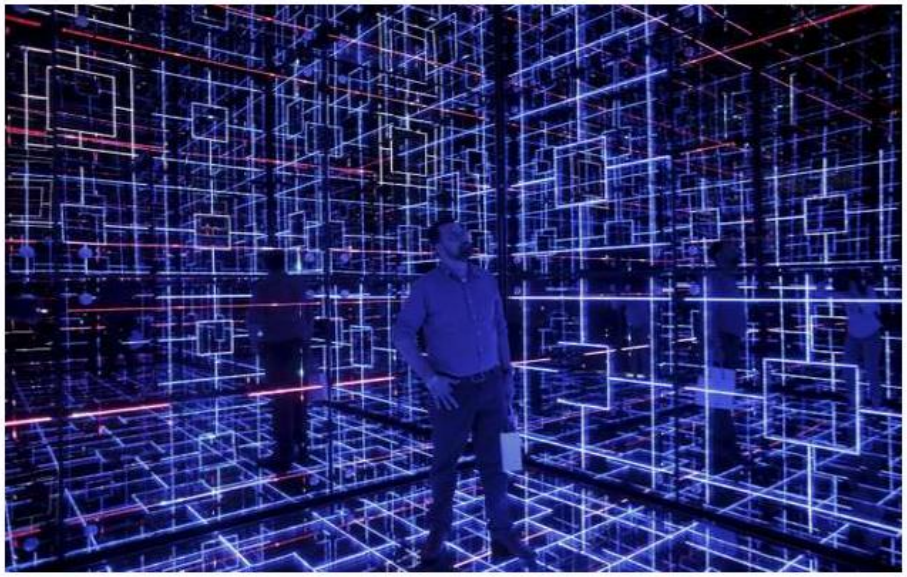
Les parades mises en place par les PMEs sont insuffisantes (quand elles existent)

Le Monde ACTUALITÉS ÉCONOMIE VIDÉOS OPINIONS CULTURE M LE MAG SERVICES

ENQUÊTE | Réservé à nos abonnés

Publié hier à 16h30, mis à jour hier à 19h09

Sensibilisés par les cyberattaques WannaCry et NotPetya en 2017, gouvernements et grandes entreprises ont réagi en créant des instances et des plans de cyberdéfense. Mais les PME restent à la traîne.

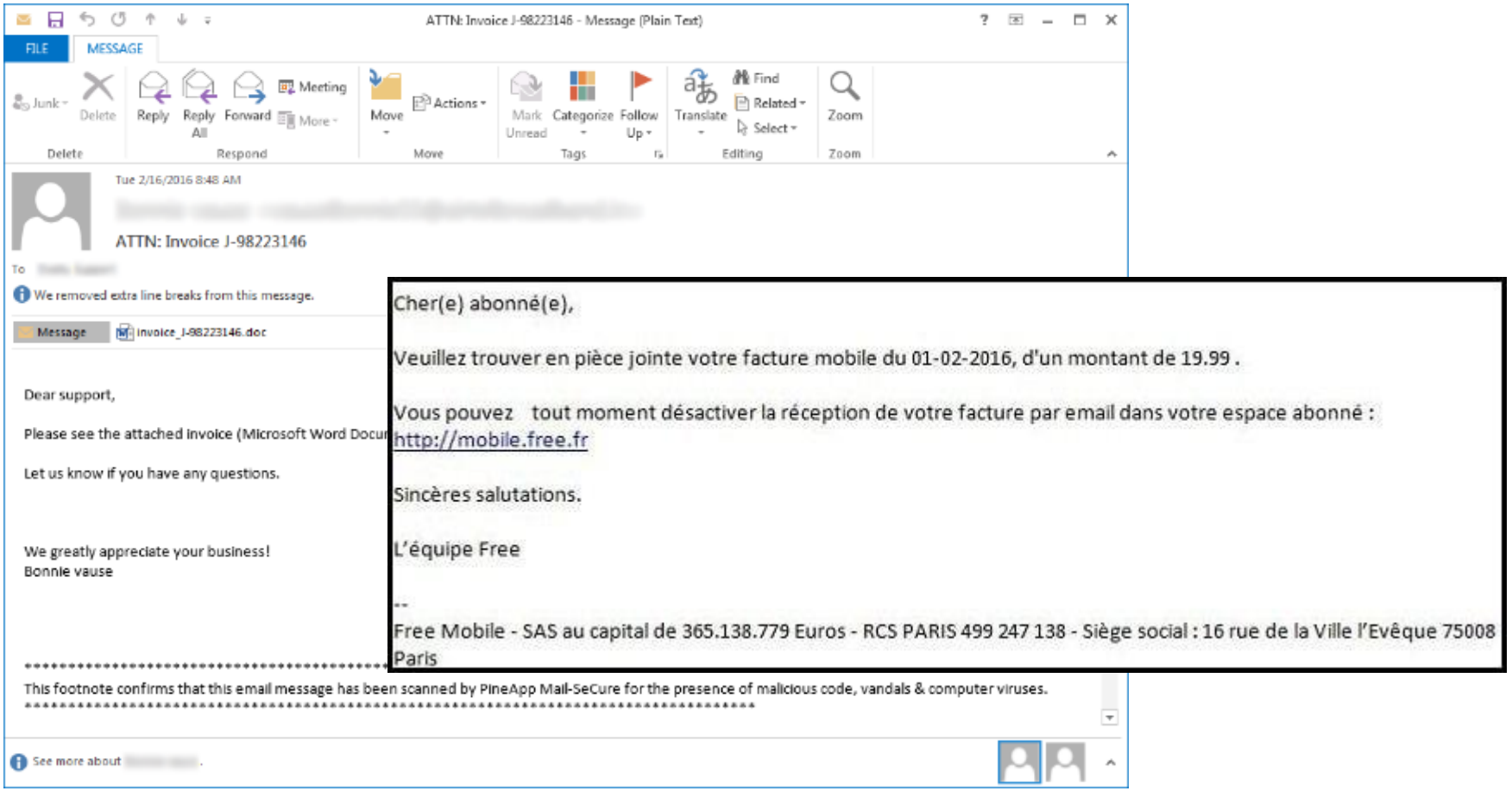


Vers un Cyber Ouragan d'attaques ?

Les TPE/PME/ETI au centre des préoccupations

Les TPE/PME/ETI sont les moins bien protégées. D'après SystemX, 50 000 PME en France sont victimes de cyberattaques, avec des conséquences parfois dramatiques (il leur est souvent impossible financièrement de se remettre d'une crise). Or, selon les chiffres de l'Insee, les TPE/PME/ETI représentent à elles-seules près de 73 % des emplois français (soit plus de 19 millions d'emplois, en 2015). Si elles sont touchées simultanément par un scénario de type "cyber ouragan", cela pourrait se transformer en une véritable crise sociétale.

En 2016, Locky avait fait un ravage en France



En Août 2018, Locky – Le Retour

****

Madame, Monsieur,

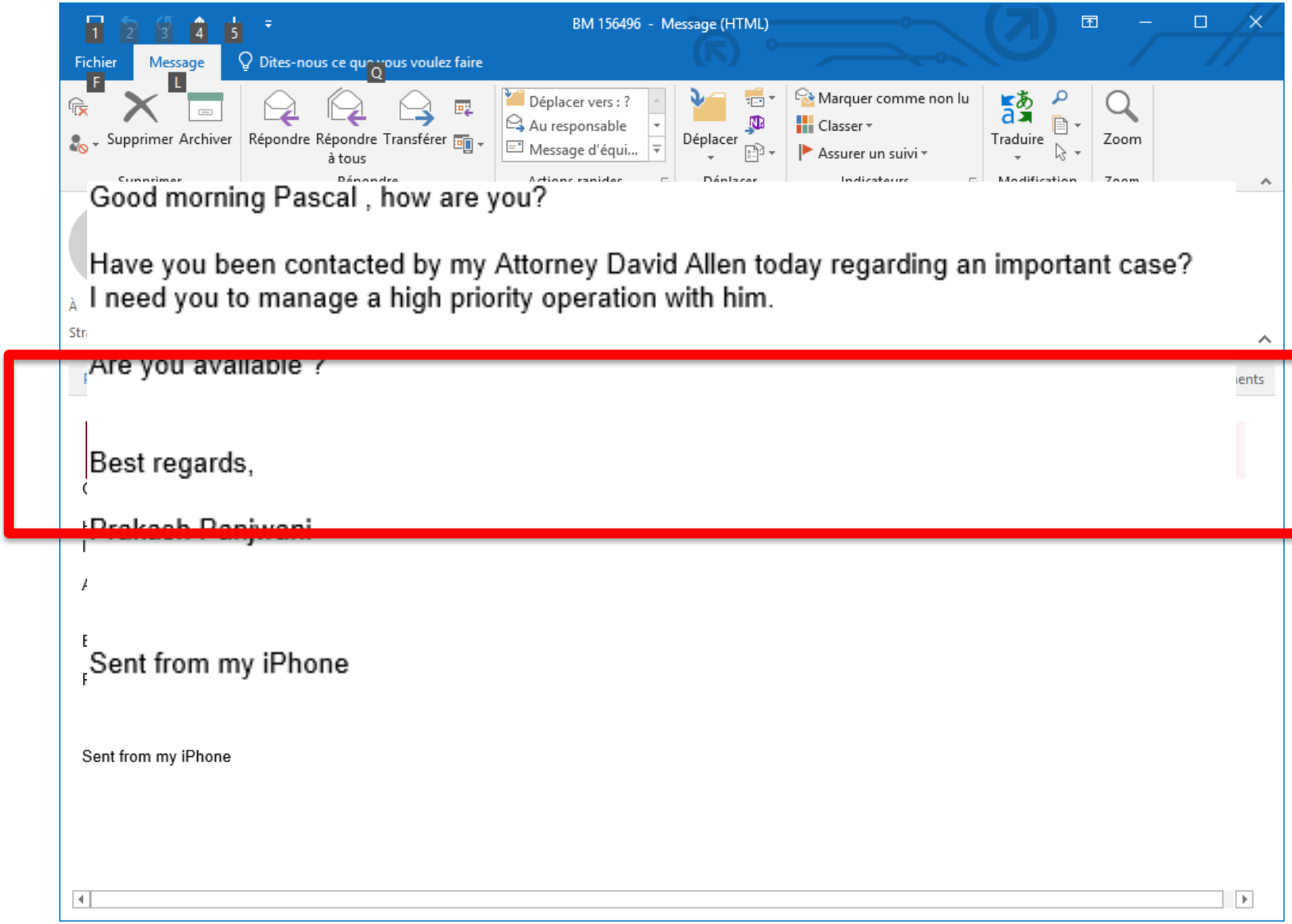
Nous vous notifions que votre commande du XX/XX/2018 d'un montant de XXX€ a bien été enregistrée.
Le contenu de votre commande est détaillé dans la facture téléchargeable en cliquant ici

Tout changement sur l'état de votre commande (préparation, expédition, etc.) vous sera automatiquement et immédiatement notifié par email.

L'expédition du produit aura lieu 24 heures au plus après le passage à l'état "validé" de votre demande.
Toute commande qui nous parvient incomplète demande des délais de traitement supplémentaires dont nous ne saurions être tenus responsables.

****

Quand le chat est plus rapide que la souris



Les auteurs du Botnet Mirai démasqués

- 3 universitaires Américains … aident maintenant le FBI pour rester hors de prison …

Mirai botnet authors avoid prison after "substantial assistance" to the FBI

Mirai botnet authors go from black hats to white hats.

By Catalin Cimpanu for Zero Day | September 19, 2018 -- 09:07 GMT (10:07 BST) | Topic: Security

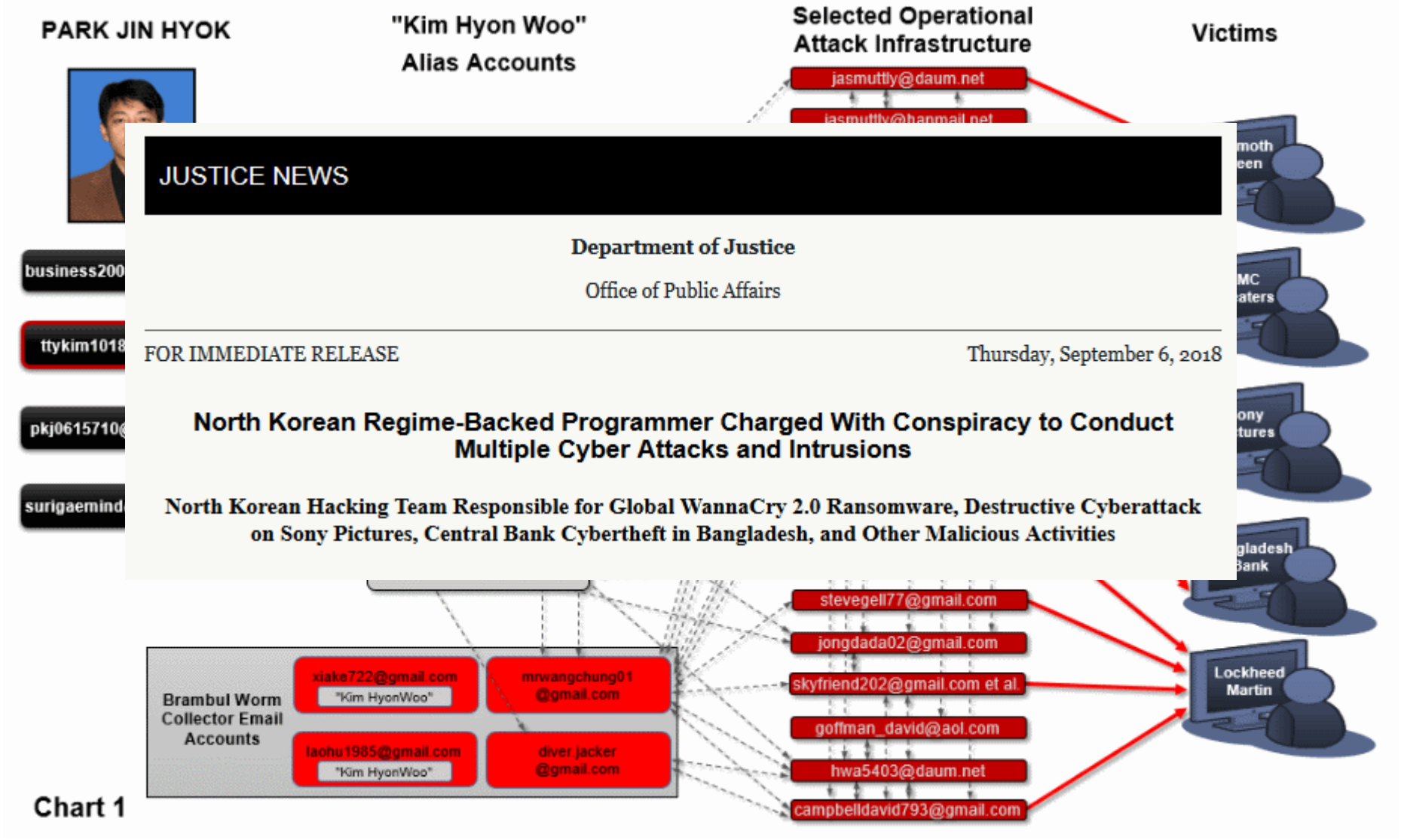
SamSam !

SamSam, le Spear-Ransomware

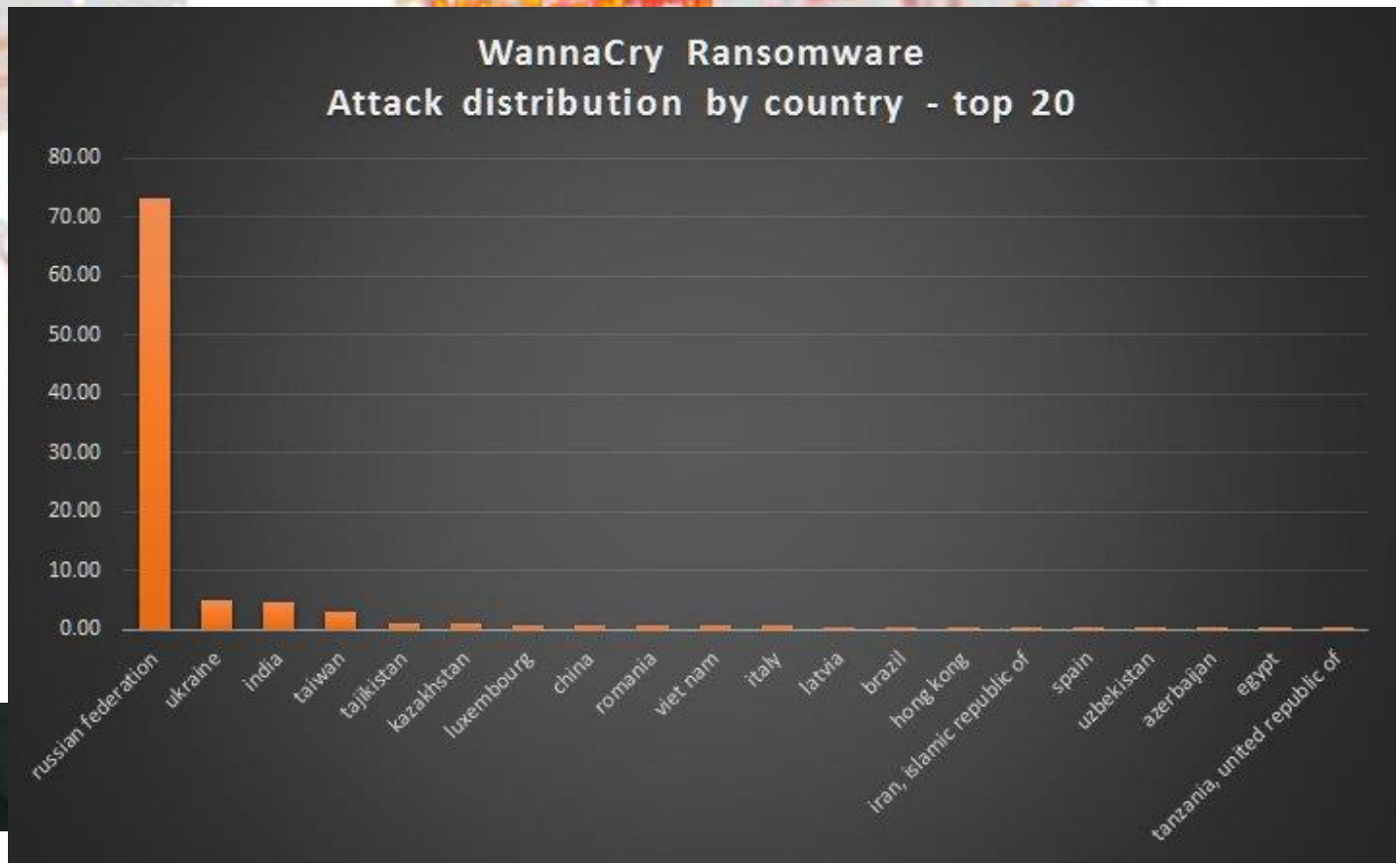
- Pas d'utilisation de Phishing
- Exploitation de vulnérabilités réseaux pour « déposer » le ransomware et le propager sur les réseaux d'entreprise (RDP)
- 6M$ récupérés / 30M$ de dommages
- Les deux Hackers sont sur la liste des pirates recherchés par le FBI mais pas arrêtés car…

en Iran.

Où en est-on avec Wannacry ?



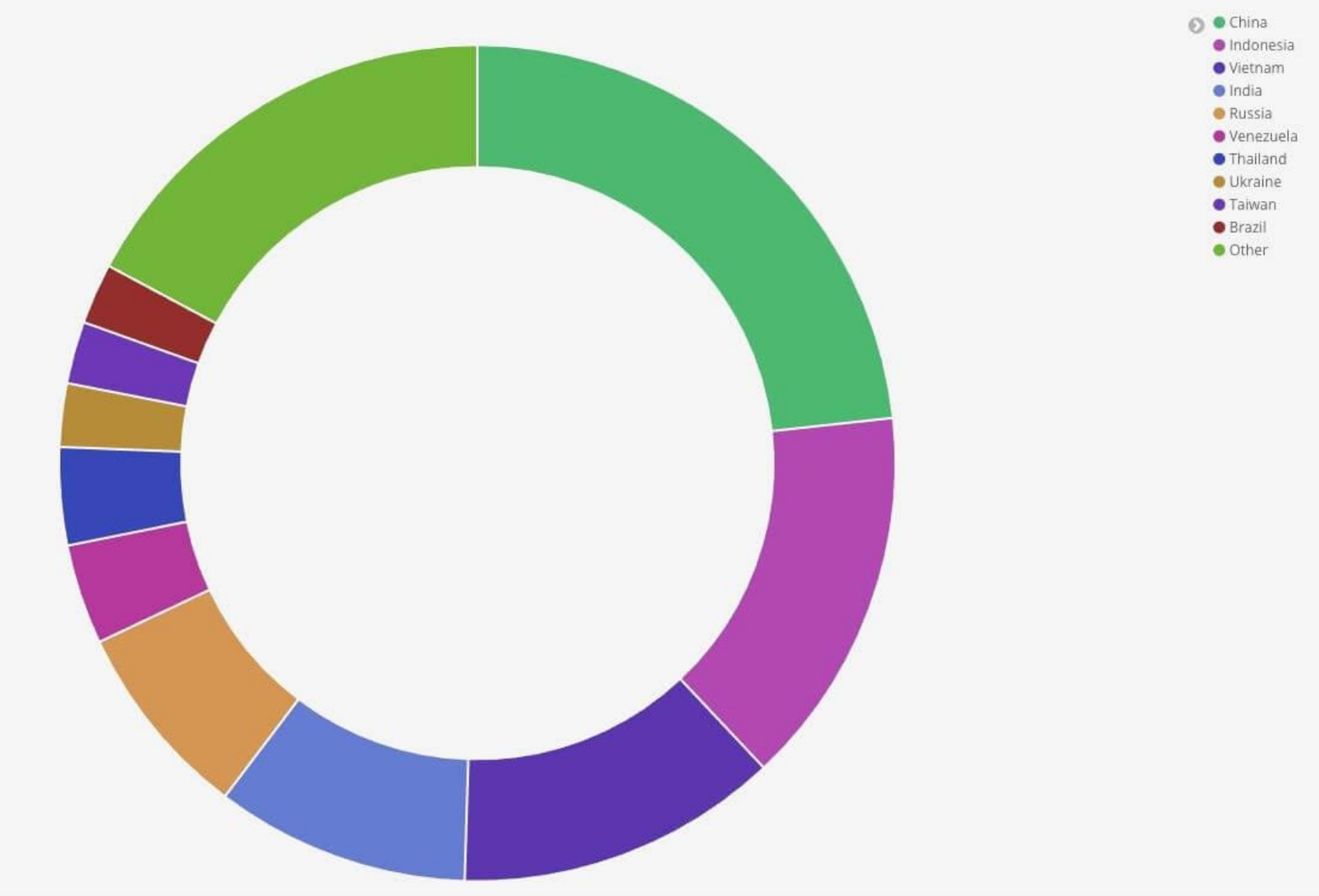
Mais bon …



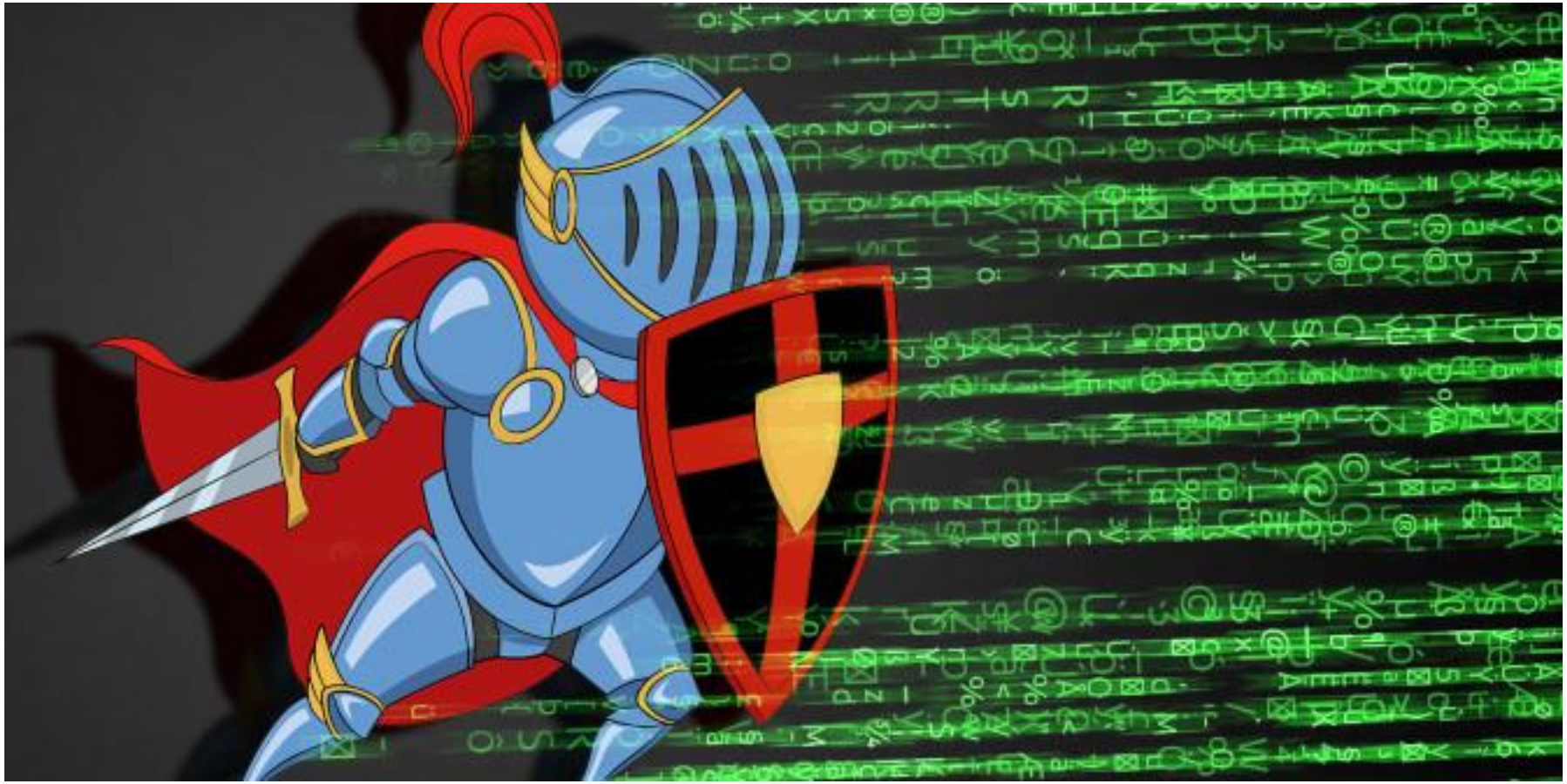
Marcus Hutchins, la malchance de la chance

- Découverte du Kill Switch par analyse du bout du code

Le Kill Switch toujours hébergé par Kryptos Logic



Imaginez une attaque de DDOS sur le Kill Switch ?



iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

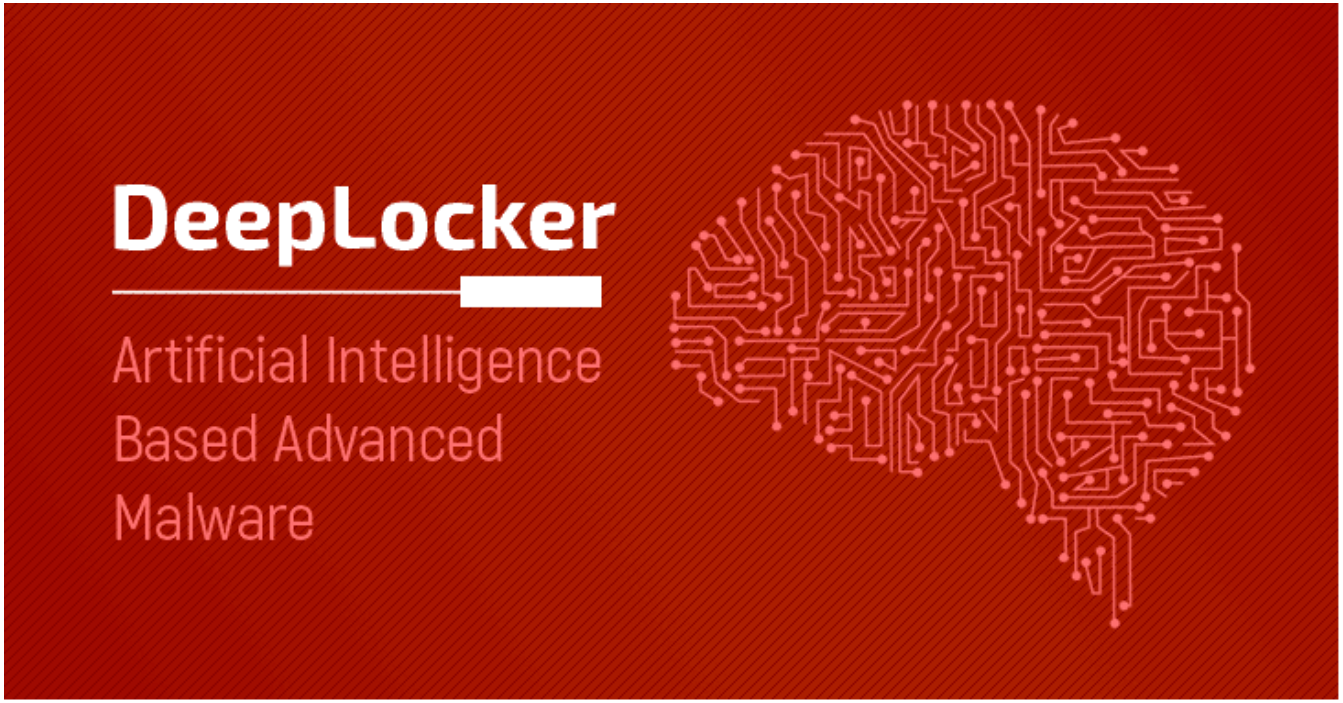
Hop Hop Hop… Kryptos… ?

Kryptos est une sculpture créée par Jim Sanborn exposée à Langley (Virginie)

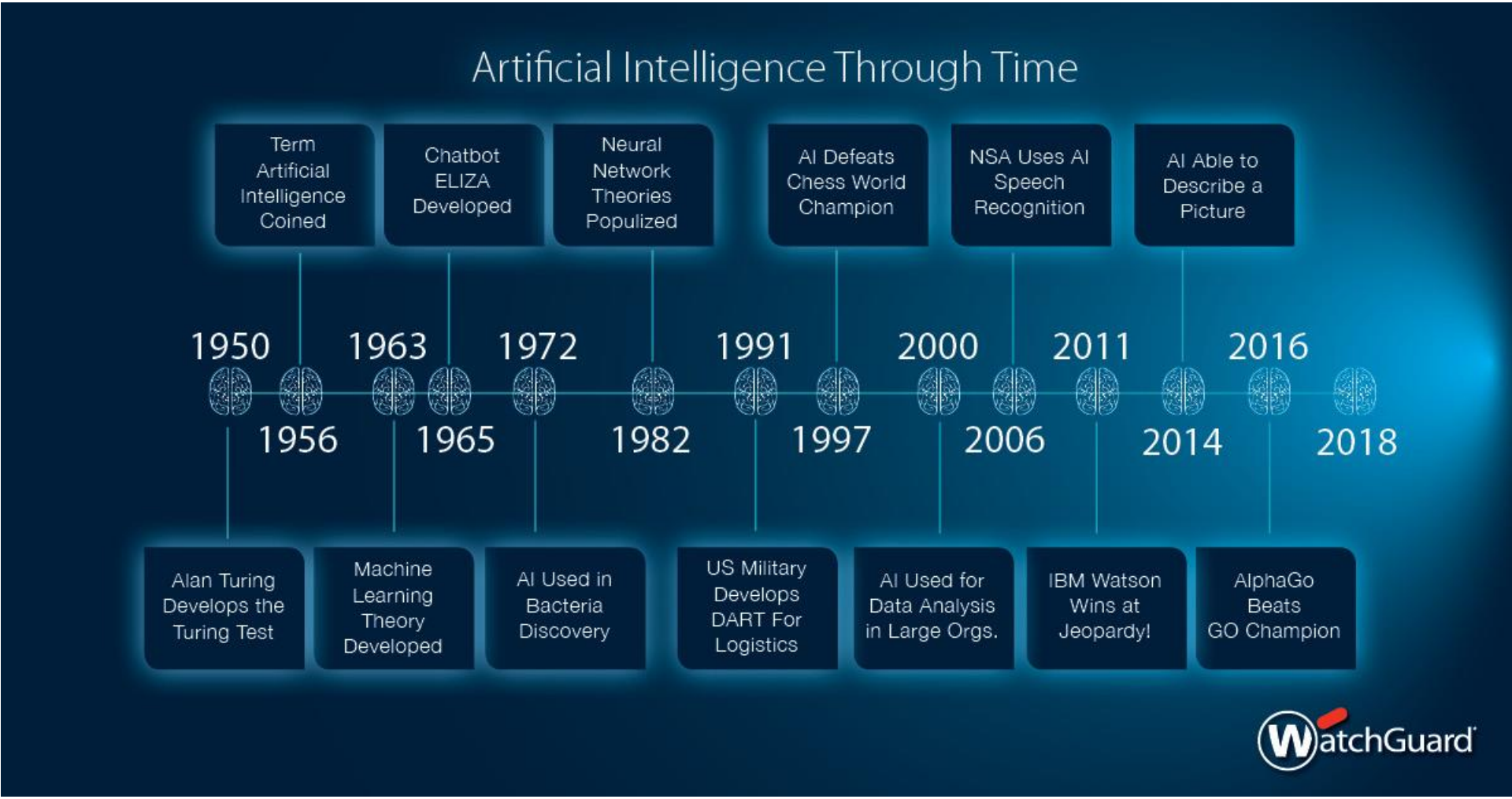
dans l'enceinte du quartier général de la **CIA**

Mais comment comprendre un code quand on ne peut plus l'analyser ?

- L'Intelligence Artificielle, au service des Pirates peut empêcher la compréhension des décisions du malware
- Démonstration faite par des chercheurs d'IBM
- Améliorant ainsi la capacité des malwares à ne pas être détectés



L'IA une nouvelle technologie ?

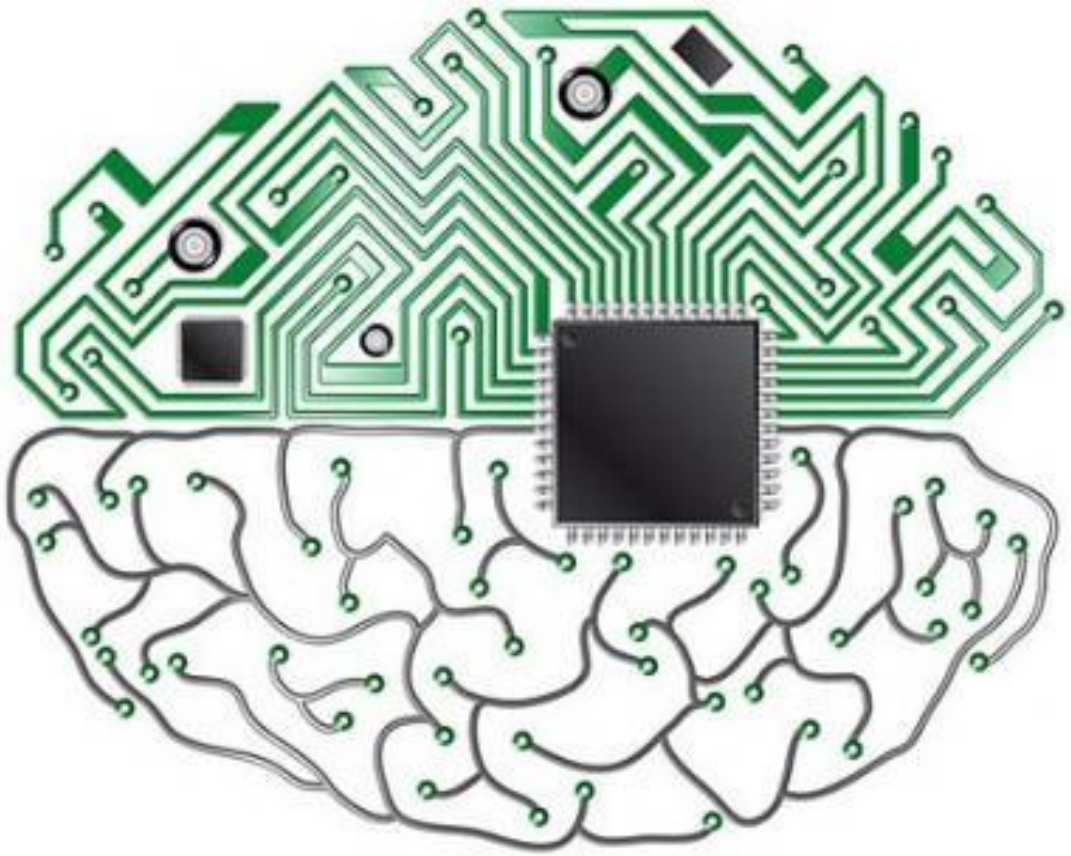


Mais c’est quoi l’Intelligence Artificielle

- Définition
  - L'intelligence artificielle (IA) est « l'ensemble des théories et des techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence »
  - Apprentissage automatique

- Utilisation
  - Battre les humains aux jeux (Echecs , Go …)
  - Reconnaissance d’images ou de paroles
  - Reconnaissance de scènes
  - Traductions
  - Pilotage Autonome
  - Comprendre vos gouts et comportements sur Internet
  - Dépistage médical

Réseaux de neurones artificiels



Apprenons ensemble…

```
1  from
2  train
3  train
4  rando
5  synap
6  for i
7      o
8      s
9  print
```

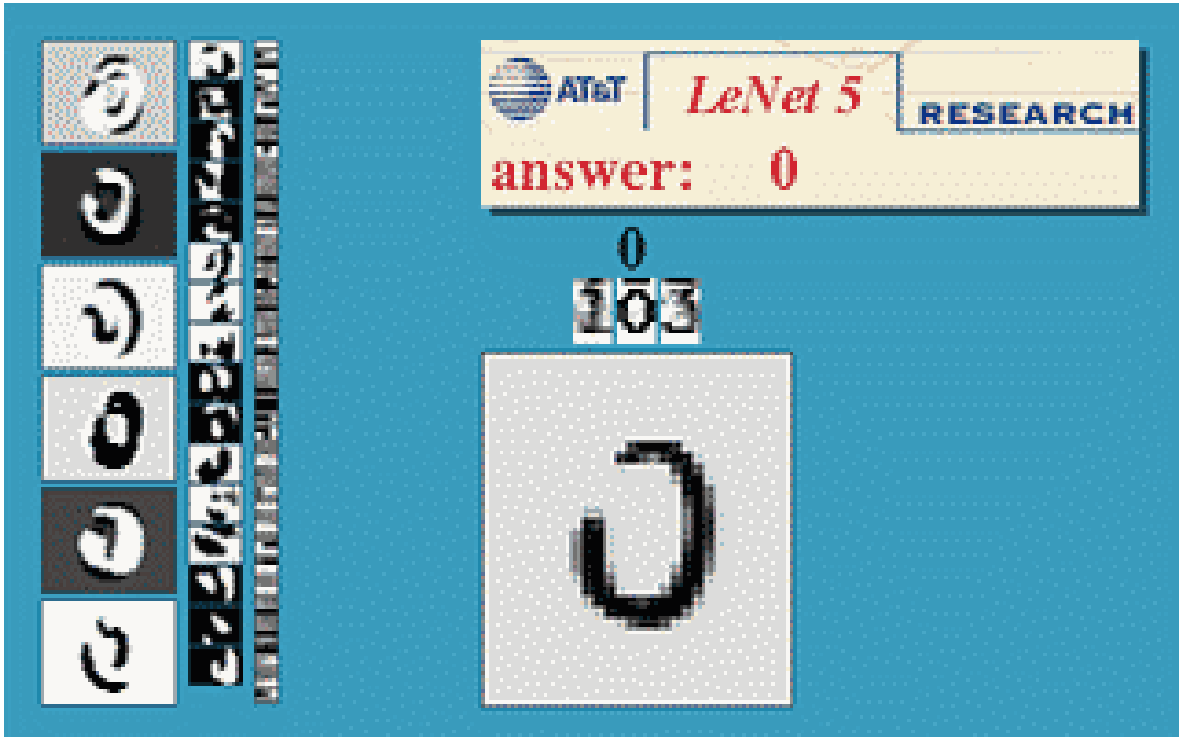
Langage Python : qu'est-ce que c'est ?

Python est un langage de programmation open source **créé par le programmeur Guido van Rossum en 1991**. Il tire son nom de l'émission Monty Python's Flying Circus.

```
out))
```

Machine Learning & Deep Learning

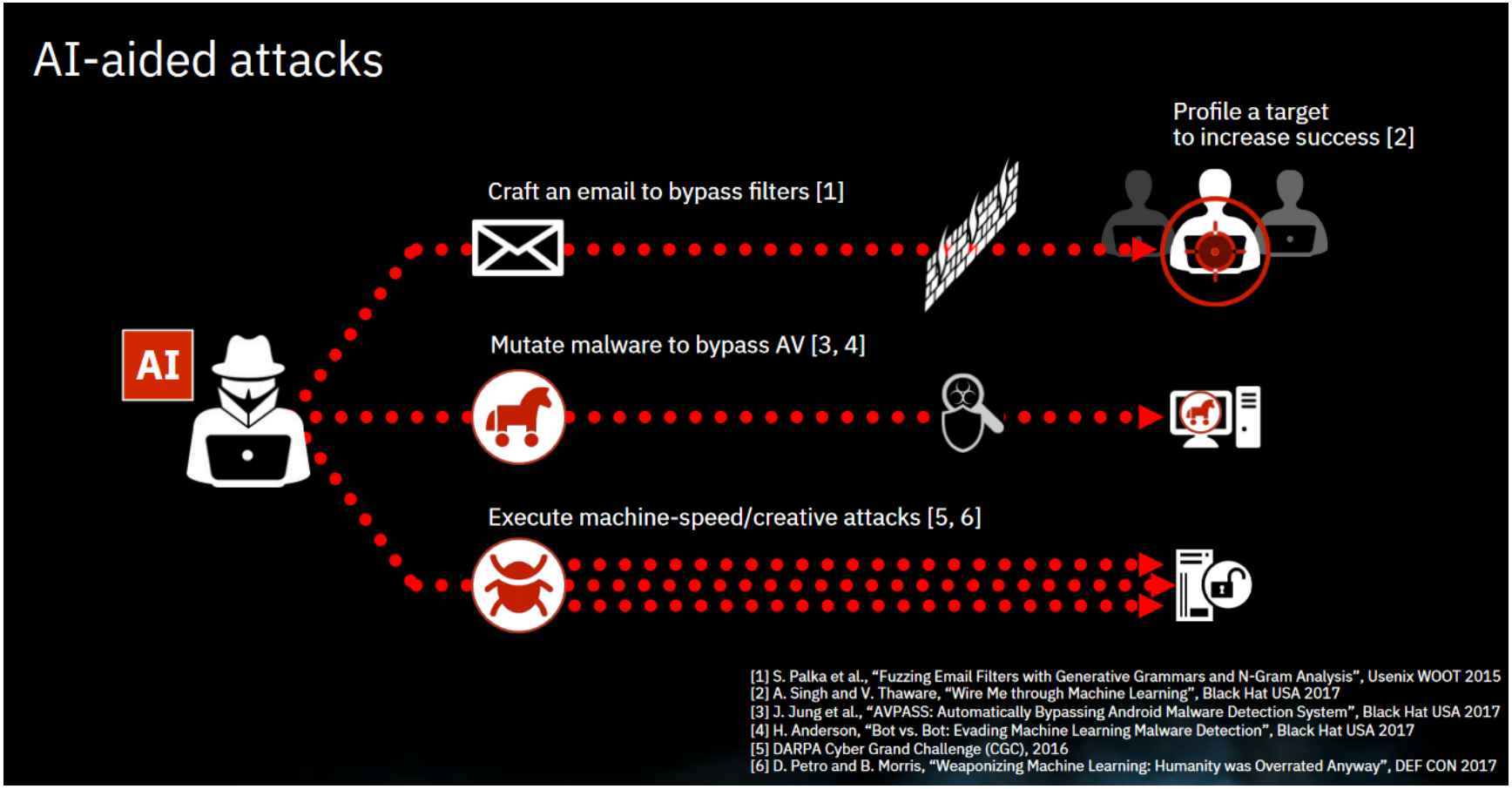
- Réseaux de neurones artificiels *profonds*
  - Capacité à trouver les attributs par l'analyse de données alors que le Machine Learning classique a besoin des données déjà décortiquées



Pourquoi parler autant de l'AI maintenant …?

- Essor du Deep Learning rendu possible par :
  - Puissance de calcul
  - Disponibilité des données (« big data »)

Ce n’est que le début des applications à la cybercriminalité

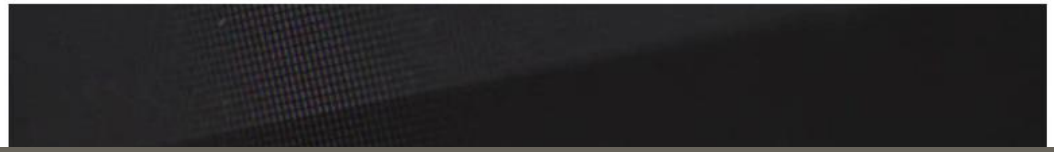


Une autre piste d'utilisation de l'IA

CYBERSÉCURITÉ INTELLIGENCE ARTIFICIELLE

PassGAN : une IA pour casser les mots de passe

PAR LOUISE MILLON - @LOUISEMILLON - 25 SEPTEMBRE 2017



Cornell University Library

arXiv.org > cs > arXiv:1709.00440

Search or A

(Help | Advanced

Computer Science > Cryptography and Security

PassGAN: A Deep Learning Approach for Password Guessing

Briland Hitaj, Paolo Gasti, Giuseppe Ateniese, Fernando Perez-Cruz

(Submitted on 1 Sep 2017 (v1), last revised 9 Mar 2018 (this version, v2))

State-of-the-art password guessing tools, such as HashCat and John the Ripper, enable users to check billions of passwords per second against password hashes. In addition to performing straightforward dictionary attacks, these tools can expand password dictionaries using password generation rules, such as concatenation of words (e.g., "password123456") and leet speak (e.g., "password" becomes "p4s5w0rd"). Although these rules work well in practice, expanding them to model further passwords is a laborious task that requires specialized expertise. To address this issue, in this paper we introduce PassGAN, a novel approach that replaces human-generated password rules with theory-grounded machine learning algorithms. Instead of relying on manual password analysis, PassGAN uses a Generative Adversarial Network (GAN) to autonomously learn the distribution of real passwords from actual password leaks, and to generate high-quality password guesses. Our experiments show that this approach is very promising. When we evaluated PassGAN on two large password datasets, we were able to surpass rule-based and state-of-the-art machine learning password guessing tools. However, in contrast with the other tools, PassGAN achieved this result without any a-priori knowledge on passwords or common password structures. Additionally, when we combined the output of PassGAN with the output of HashCat, we were able to match 51%-73% more passwords than with HashCat alone. This is remarkable, because it shows that PassGAN can autonomously extract a considerable number of password properties that current state-of-the art rules do not encode.

Le Big Data des Mots de Passe

DarkNet : Découverte d'
de 1,4 milliards d'identif
passe en clair

12 décembre 2017 - 1 commentaire - Temps de lecture : 1 m

LE FIGARO.fr
tech & web

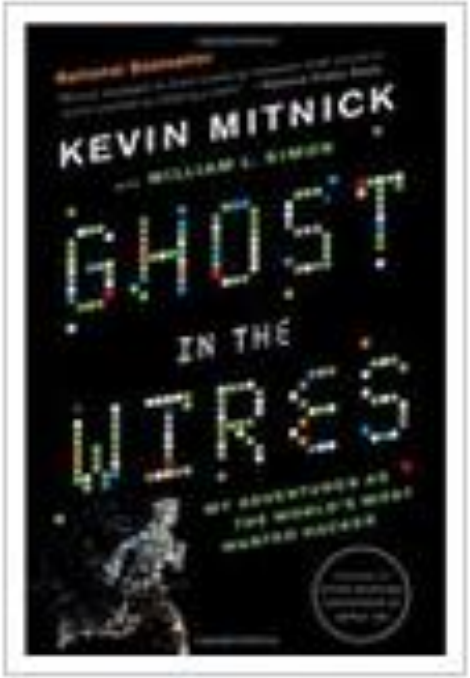
› Tech & Web

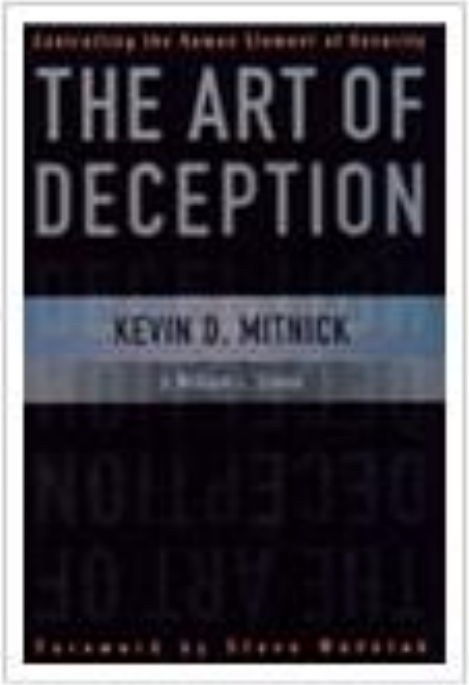
Plus de 100 millions de mots de passe LinkedIn dans la nature

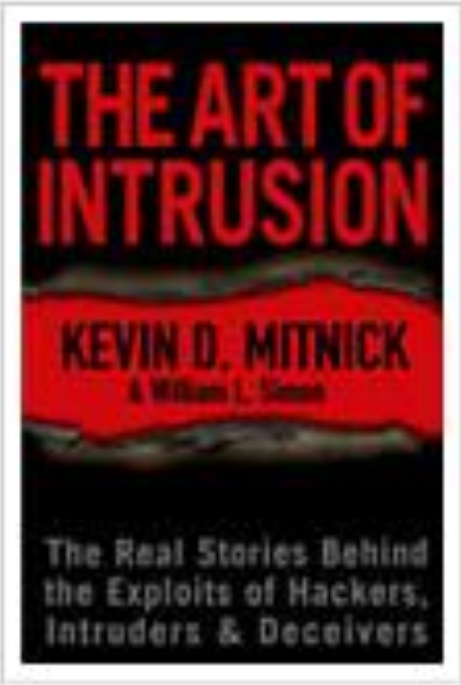
Par Benjamin Ferran | Mis à jour le 18/05/2016 à 21:39 / Publié le 18/05/2016 à 18:07

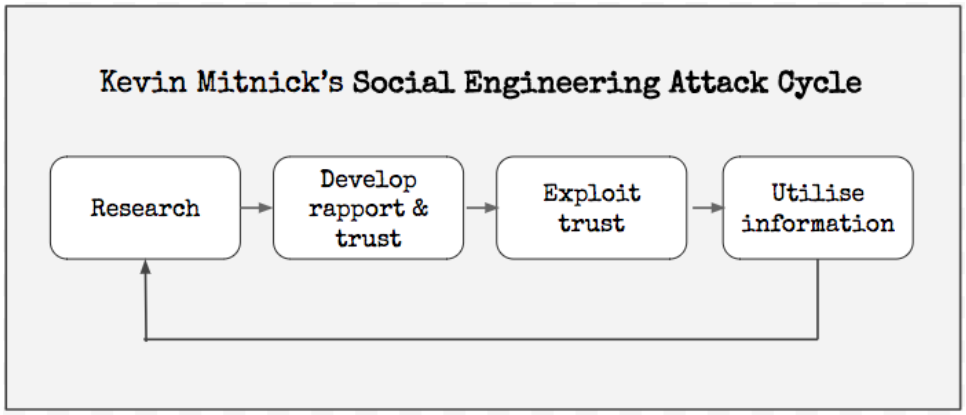
Biométrie… l'ultime sécurité?

Le Moment Culture – Kevin Mitnick









Et il y aura toujours un « exploit » …

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

economie.gouv.fr
Le portail de l'Économie, des Finances, de l'Action et des Comptes publics

Lettres d'information

Accueil | Particuliers | Entreprises | Les ministres | Les ministères | Presse

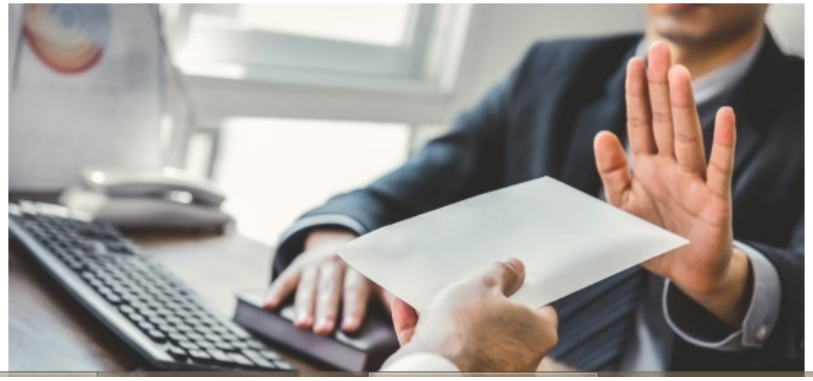
A+ A−

Accueil du portail ▸ Entreprises ▸ RGPD : attention aux arnaques !

RGPD : attention aux arnaques !

05/07/2018

Depuis le 25 mai 2018, les professionnels collectant des données sur leurs clients ou leurs abonnés sont tenus de se conformer au Règlement général de la protection des données (RGPD). Ce règlement européen a pour objectif d'encadrer de traitement des données. Pour les aider, des entreprises peuvent les accompagner. Mais attention aux offres frauduleuses !



Placer le curseur de la sécurité au plus haut

WATCHGUARD DIMENSION

HOST RANSOMWARE PRVENTION (HRP)

DNS WATCH

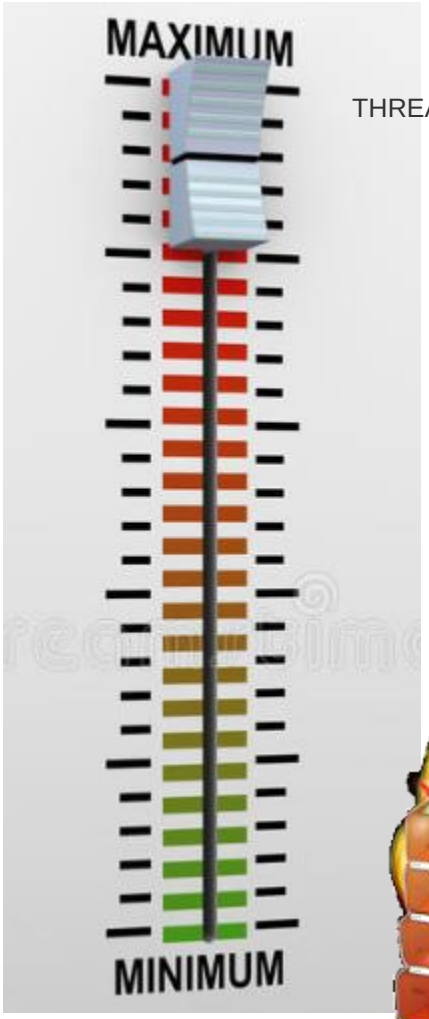
APT BLOCKER

REPUTATION ENABLED DEFENSE SERVICE (RED)

NETWORK DISCOVERY

INTRUSION PREVENTION SERVICE (IPS)

WEBBLOCKER



THREAT DETECTION & RESPONSE

INTELLIGENT AV

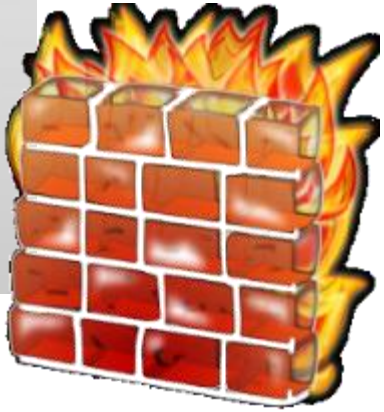
DATA LOSS PREVENTION (DLP)

ACCESS PORTAL (Clientless VPN)

BOTNET DETECTION

APPLICATION CONTROL

GATEWAY ANTIVIRUS (GAV)



SPAMBLOCKER

Les Suites de Sécurité WatchGuard

Fonctionnalités et services	TOTAL SECURITY SUITE	Basic Security Suite
Service de prévention d'intrusions (IPS)	✓	✓
Contrôle d'application	✓	✓
WebBlocker (filtrage d'URL)	✓	✓
spamBlocker (antispam)	✓	✓
Gateway AntiVirus (Antivirus de passerelle)	✓	✓
Reputation Enabled Defense (RED, Autorité de réputation)	✓	✓
Network Discovery (Découverte réseau)	✓	✓
APT Blocker	✓	
Protection contre les pertes de données (Data Loss Protection, DLP)	✓	
Threat Detection and Response	✓	
DNSWatch	✓	
Access Portal*	✓	
IntelligentAV*	✓	
Dimension Command	✓	
Support	Gold (24 h/24, 7 j/7)	Standard (24 h/24, 7 j/7)

Disponible sur les Firebox Série-M de dernière génération

La Total Security Suite, c'est être armé pour le jeu du chat et de la souris

Merci !