

INTRODUCTION À LA SÉCURITÉ INFORMATIQUE SÉANCE 4

Marc-Olivier Killijian

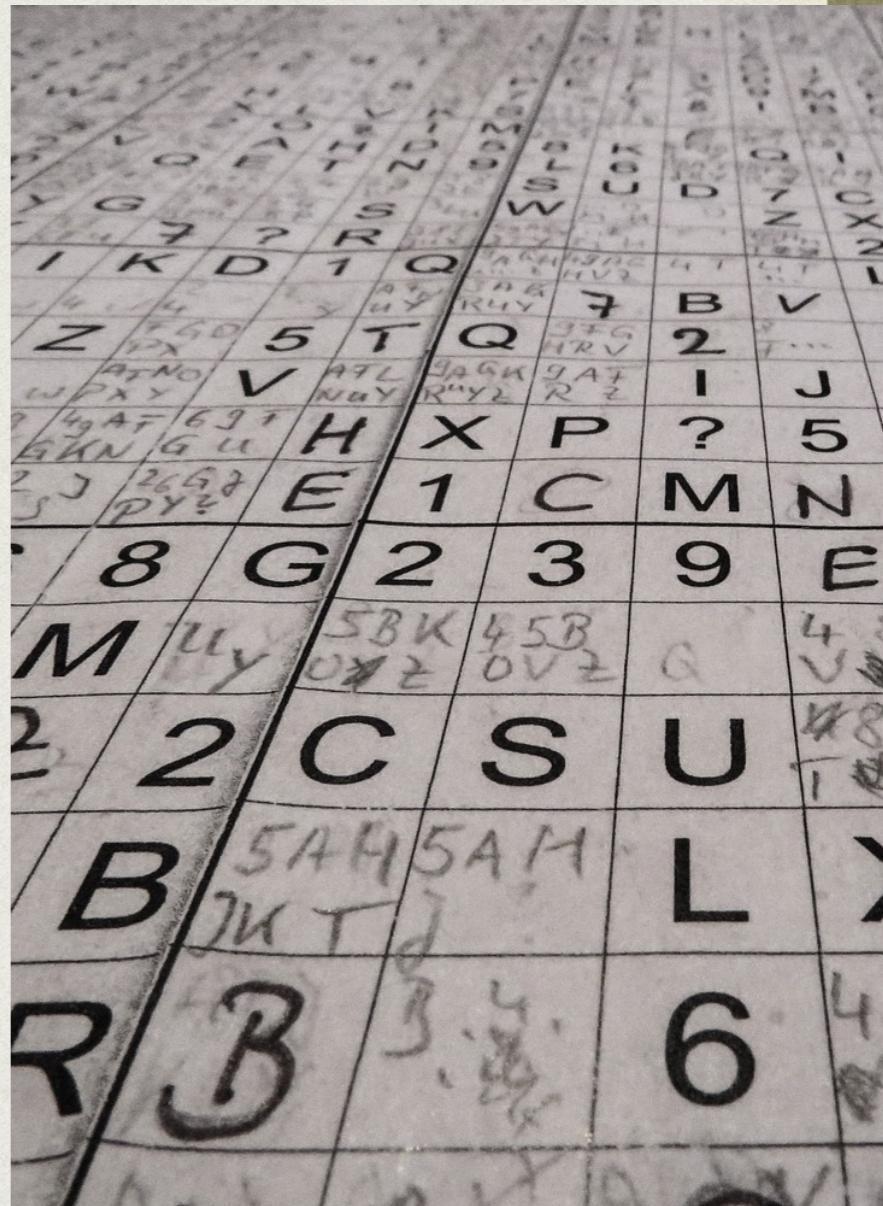
UQAM, CNRS

INF4471 A21

ANALYSE DE RISQUES

LA DIFFICULTÉ DE LA SÉCURITÉ INFORMATIQUE

- **Infaillibilité**
pour de nombreuses attaques, l'attaquant n'a besoin que de réussir **1 seule fois**
- **Ubiquité**
Postes: actualiser et migrer SEs et apps
Infrastructure réseau: actualiser (matériel, firmware, SEs, configurations) et surveiller (débits, flux)
Utilisateurs: actualiser (rôles, départs/arrivées, droits), sensibiliser, surveiller (mdp, accès)
Logiciels métiers, logiciels de sécurité, etc.
- **Tout savoir**
Faire de la veille sur tout ces points
Avoir tout prévu (ou plutôt que personne ne pense à quelque-chose que l'on n'a pas prévu)
- **Energie infinie**
Les attaquants ont une portée planétaire (pas d'horaire)
... sont nombreux
... n'ont rien d'autre à faire
... sont teigneux et passionnés



PRINCIPE DE BASE

- L'attaquant gagnera
 - A. Jamais
 - B. Lorsque je serais mort
 - C. Toujours
 - D. De la prison

PRINCIPE DE BASE

- L'attaquant gagnera
 - A. Jamais
 - B. Lorsque je serais mort
 - C. Toujours**
 - D. De la prison

PRINCIPE DE BASE (2)

- Vu qu'on va perdre, autant
 - A. Ne pas se défendre
 - B. S'y préparer
 - C. Changer de job

PRINCIPE DE BASE (2)

- Vu qu'on va perdre, autant
 - A. Ne pas se défendre
 - B. S'y préparer
 - C. Changer de job

PRINCIPE DE BASE (2)

- Vu qu'on va perdre, autant
 - A. Ne pas se défendre
 - B. S'y préparer**
 - C. Changer de job

SE PRÉPARER AU PIRE

- Si la dernière barrière tombe ?
 - Puis-je revenir en arrière (sauvegardes) ?
 - Puis-je tout couper ?
 - Qui dois-je prévenir ?
 - Quel protocole pour revenir à une situation normale ?
- Et dans ce cas
 - Quelle est l'**étendue des dégâts** ?
 - Combien de temps avant **recouvrement** ?
 - Comment couvrir ses **pertes** ?



ANALYSE DE RISQUE (1)

- L'analyse de risque, des risque, du risque, l'appréciation des risques
- c'est **préparer** son organisation, son entreprise, son système d'information **à une attaque**
- **identifier les actifs, les menaces et vulnérabilités**
- **évaluer les risques**
- **identifier des solutions** et les prioriser
- **auditer et recommencer**

ANALYSE DE RISQUE (2)

- identifier des solutions
 - définir des **politiques de sécurité** (acteurs, rôles, services, droits)
 - mettre en place une **organisation de la sécurité** (responsables, protocoles)
 - définir des **plans de recouvrement** (comment on fait quand le SI est ou est en train de tomber?)
 - prévoir une **réponse à incident** (les attaquants sont-ils encore là? de quelles bases saines on dispose? que fait-on si on trouve qui a attaqué? etc.)
 - **former** les usagers

ANALYSE DE RISQUE (2)

- identifier des solutions
 - définir des **politiques de sécurité** (acteurs, rôles, services, droits)
 - mettre en place une **organisation de la sécurité** (responsables, protocoles)
 - définir des **plans de recouvrement** (comment on fait quand le SI est ou est en train de tomber?)
 - prévoir une **réponse à incident** (les attaquants sont-ils encore là? de quelles bases saines on dispose? que fait-on si on trouve qui a attaqué? etc.)
 - **former les usagers**

Sans ça, ça peut prendre des mois !!!

ANALYSE DE RISQUE (3)

- Ce n'est pas facile, ça peut paraître ennuyeux, mais c'est **essentiel** dans une entreprise, moyenne ou grande
- On peut facilement **passer à côté** de quelque-chose
- Alors il y a des **méthodes** pour nous guider, beaucoup de méthodes
 - CRAMM, EBIOS, Mehari, TIK, Octave, etc.
- Et des **normes**, beaucoup de normes...
 - ISO 27000 et **27001**, ISO 13335, ISO 15408, ISO 17799, ISO 21287
- Mais on s'en dans les activités de la semaine vous allez regarder **EBIOS-RM** (efficace, pratique, gratuite, adaptable) et vous aurez une bonne idée de ce à quoi peuvent ressembler les autres.

FRAUDE SUR INTERNET/ ATTAQUES

HAMEÇONNAGE

PETITS ET GROS POISSONS

- **Phishing, hameçonnage** : technique générale et largement utilisée (appât)
 - utiliser un **courriel frauduleux**, en se faisant passer pour quelqu'un d'autre, inspirant **confiance**, afin de récupérer les **identifiants** d'un utilisateur et (souvent) faire une **usurpation d'identité**
- **Spear-phishing, harponnage** : variante ciblée
 - phishing + ingénierie sociale pour **VIP**
- **Whaling, chasse à la baleine** : variante ciblée
 - pour super VIP



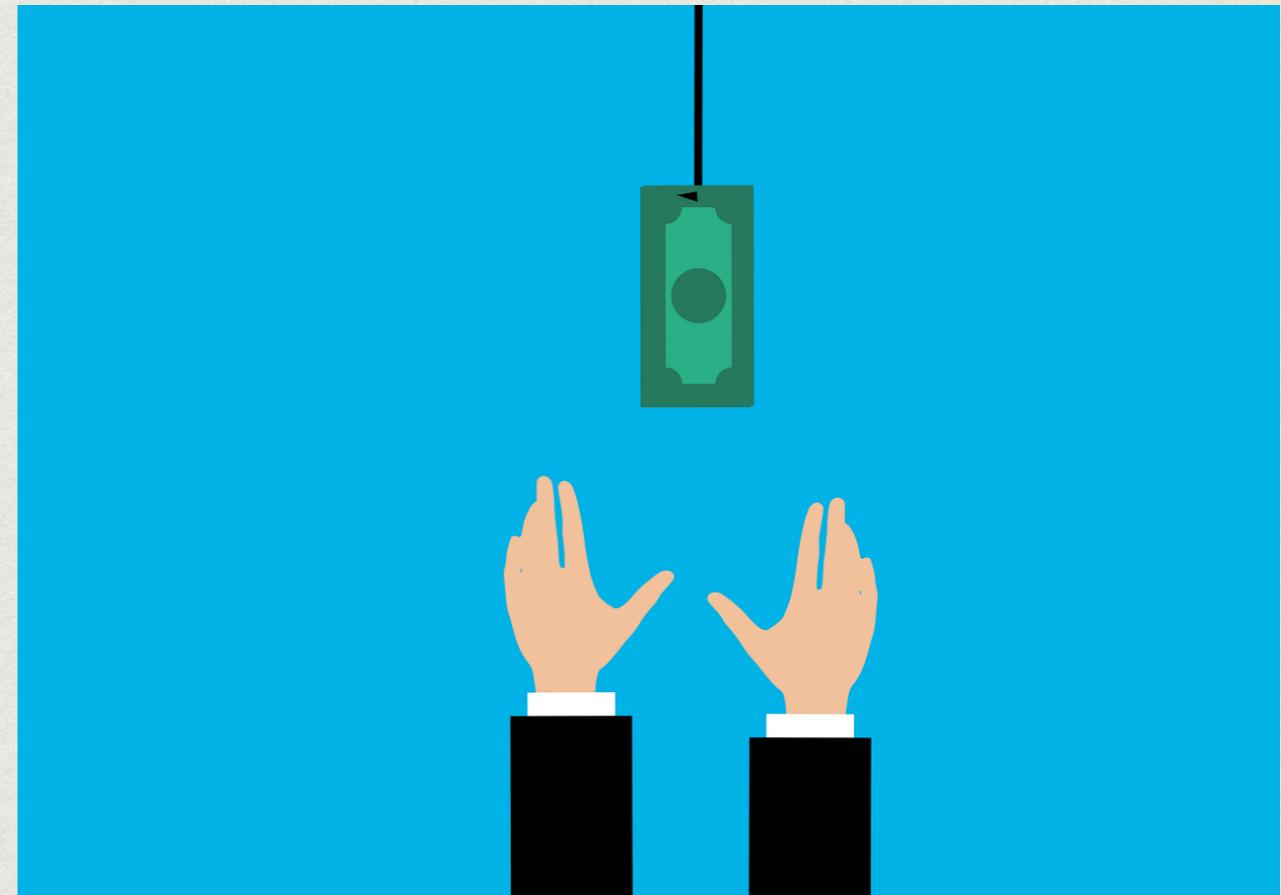
OBJECTIFS

- Obtenir des **credentials**
 - login/password
 - copies de documents d'identité
 - NAS, #carte de crédit
- Pour ensuite monter des **attaques plus avancées**
 - arnaque crédit, fraude carte de crédit, vols d'identité, attaque ciblée sur une société, etc.
- Installer un **malware**



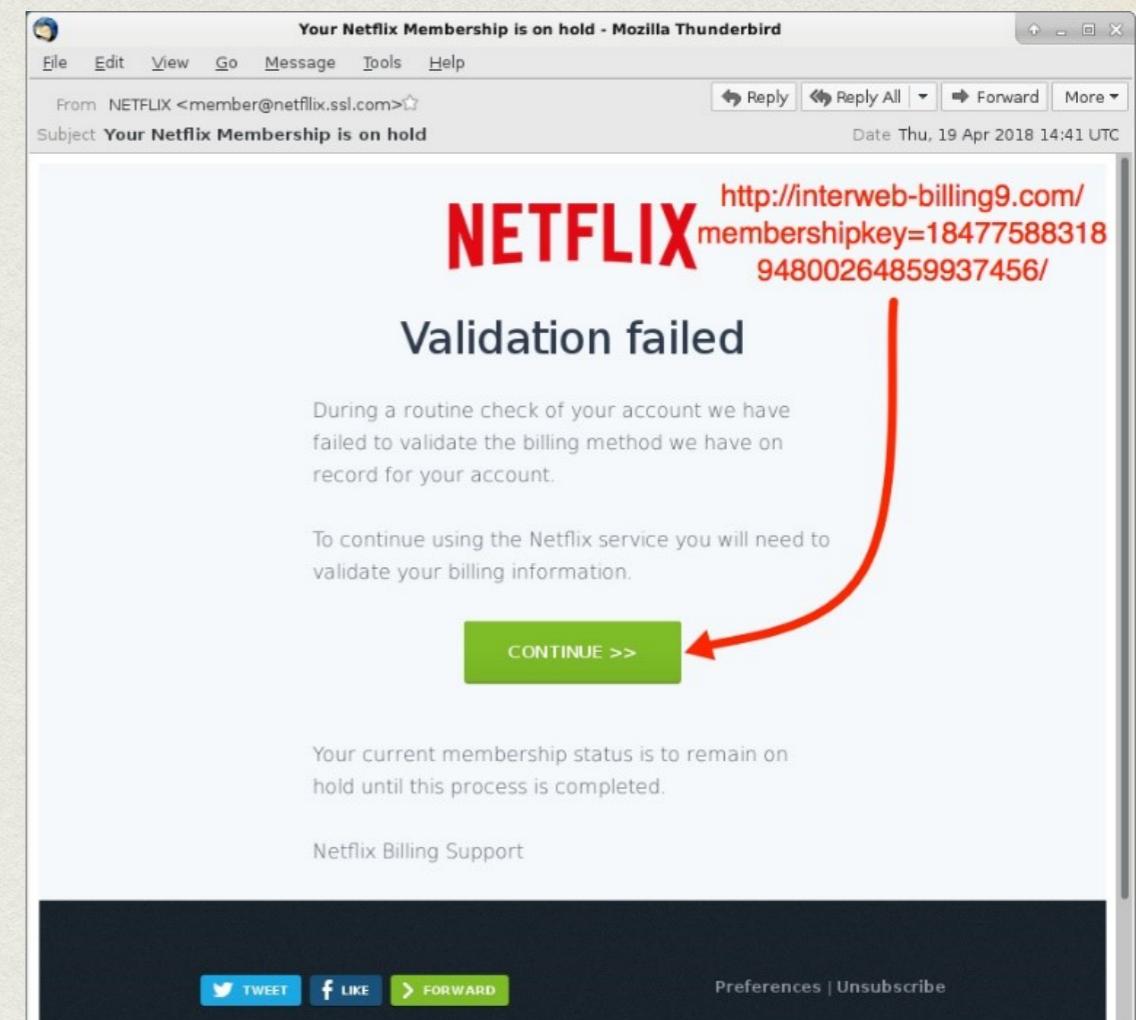
TOUS LES MOYENS SONT BONS

- **Courriels** mais ne passent pas forcément les antispam, antivirus, etc.
- **Autre moyens :**
 - Textos, messageries (Messenger, etc.)
 - Appels téléphoniques (ex. NAS)
 - Visites à domicile



COURRIELS

- **Classiques** : boite courriel pleine, loterie ou cadeaux gagnés, argent à sortir d'un pays (*scam*), etc.
- Avant : yavé des grausse fotes dortograf ; envoyés d'@ peu orthodoxes
 - **C'est de moins en moins vrai**
 - **Il existe des kits de phishing pro (liste d'adresses mail, serveurs d'envoi spam, hébergement scams, formation, blanchiment d'argent, etc.)**
- Envoyés d'adresses déguisées : ex. gimletmedia -> gimletrmedia
- Contient des **attachements ou des liens suspects**
 - fichiers qui embarquent un **malware** (pdf, doc, exe, etc.)
 - liens (souvent cachés derrière une image) qui emmènent sur une **réplique malveillante de site institutionnel** (adresses déguisées ou pas)



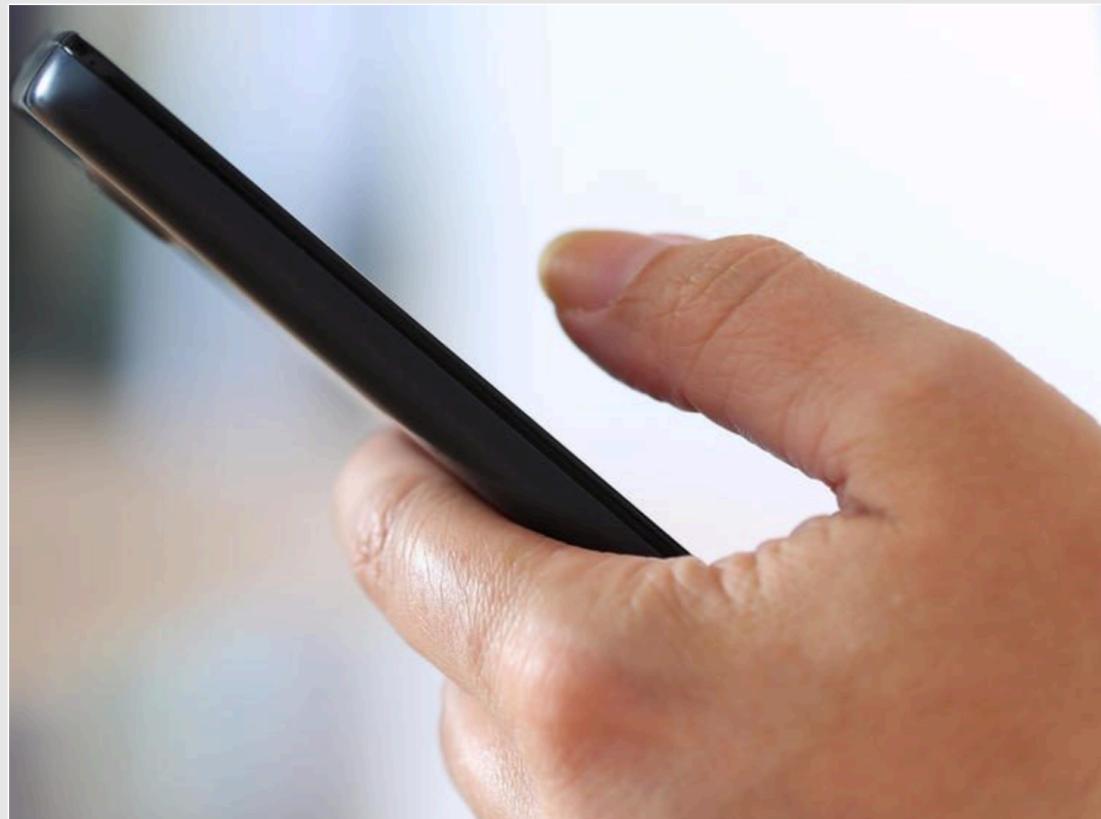
APPELS

Gare aux appels frauduleux concernant votre numéro d'assurance sociale!

Le 7 juillet 2020 – Modifié à 14 h 29 min le 7 juillet 2020

Temps de lecture : 1 min 30 s

Communiqué



(Photo : depositphotos.com)

Le Service de police de Thetford Mines désire mettre en garde la population qu'un stratagème de fraude téléphonique semble commencer sur le territoire. La Sûreté municipale note une augmentation du nombre d'appels où des fraudeurs font croire aux victimes que leur numéro d'assurance sociale (NAS) est bloqué, compromis ou suspendu. Rien de cela n'est vrai.

Selon le Centre antifraude du Canada, les fraudeurs peuvent ajouter que cela est lié à une activité frauduleuse ou criminelle et demanderaient aux victimes de fournir leur NAS et d'autres renseignements personnels et financiers (date de naissance, nom, adresse, soldes de comptes, etc.). Or, les personnes qui s'exécutent risquent d'être victimes de fraude à l'identité.



Securing today
and tomorrow

Phone Scam Alert – 60 second version

Voice over: New message.

Scammer message: Department of the Social Security Administration. The reason of this call is to inform you that your Social Security number has been suspended for suspicion of illegal activity.

If you do not contact us immediately, your account will be deactivated.

For more information about this case file, press 1 or call immediately our department number 326--

Announcer: This is a scam!

ESCROQUERIE TWITTER

JUILLET 2020

- Investissements en bitcoin
 - Scam 116,000US\$
- Ingénierie sociale pour obtenir **credentials admin Twitter**
- **Contrôle compte baleines** (E.Musk, B.Gates, B.Obama, etc.)

DigitalNewsDaily

Twitter Reeling From Hacker Attack

by Gavin O'Malley @mp_gavin, July 16, 2020



With its reputation on the line, Twitter is struggling to explain a major security breach that briefly gave hackers control over the accounts of Joe Biden, Elon Musk, Bill Gates and other high-profile figures.

"Tough day for us at Twitter," cofounder-CEO Jack Dorsey tweeted on Wednesday night. "We all feel terrible this happened."

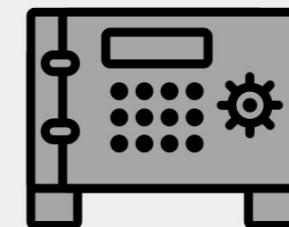
Officially, the company said it detected what it believes was a "coordinated social engineering attack" by people who successfully targeted some of its employees with access to internal systems and tools.

"We know they used this access to take control of many highly-visible (including verified) accounts and Tweet on their behalf," the company tweeted on

VOL D'IDENTITÉ

OBJECTIFS

- Se faire **passer pour un individu** pour obtenir un **bénéfice en son nom**
 - obtenir un **prêt**, une carte de **crédit**, une ligne téléphonique, etc.
 - un **bénéfice social** (assurance santé, PCU, etc.)
 - pour monter une **autre attaque** (spear-fishing par exemple)



**PROTÉGEZ
VOTRE NAS.
PROTÉGEZ VOTRE
IDENTITÉ.**

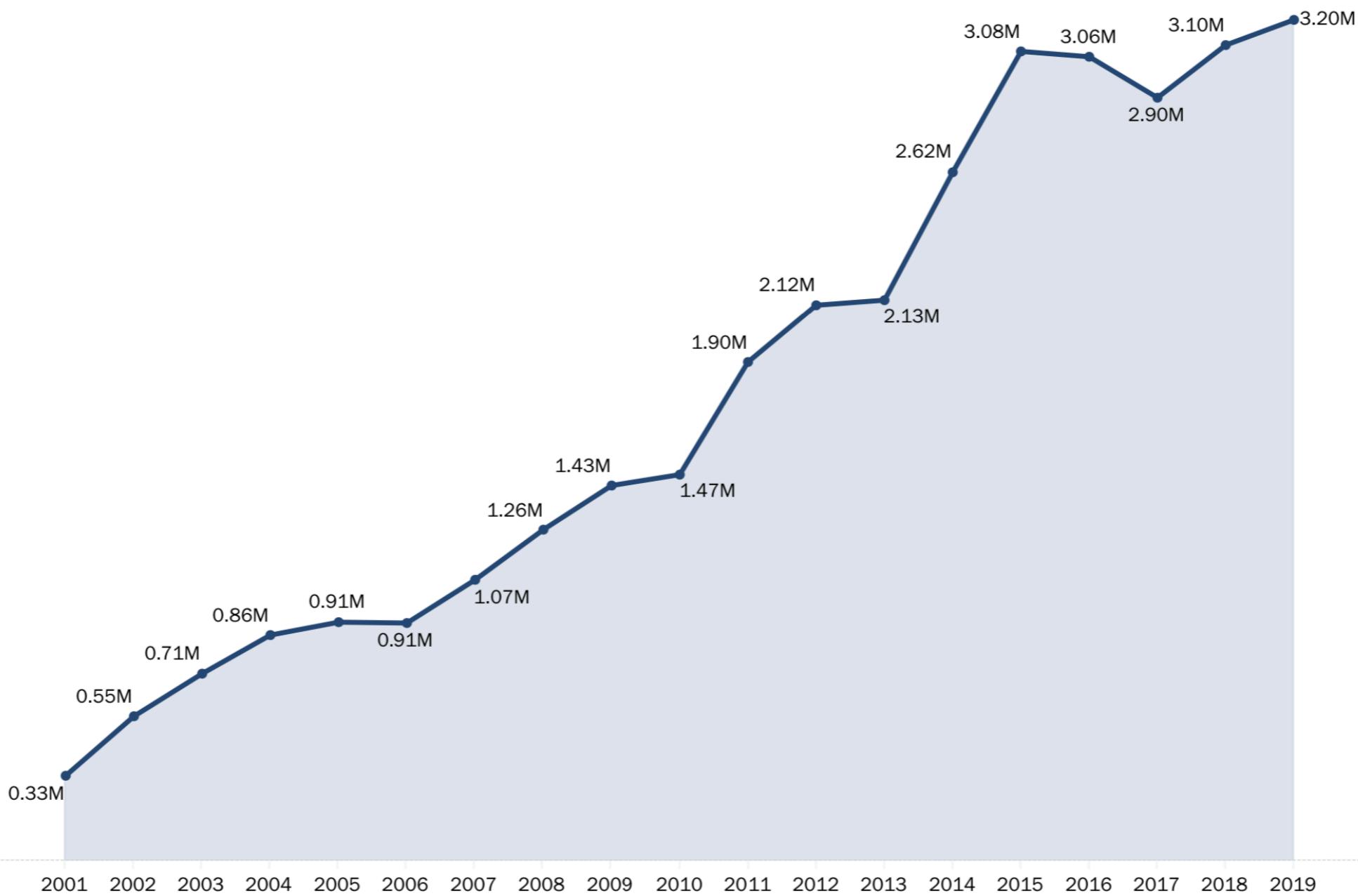
Canada

MOYENS

- Hameçonnage
- Récupération d'information sur réseaux sociaux
- Ingénierie sociale
- Skimming de cartes
- Vol de cookies

UN GRAND CLASSIQUE

Number of Fraud, Identity Theft and Other Reports by Year



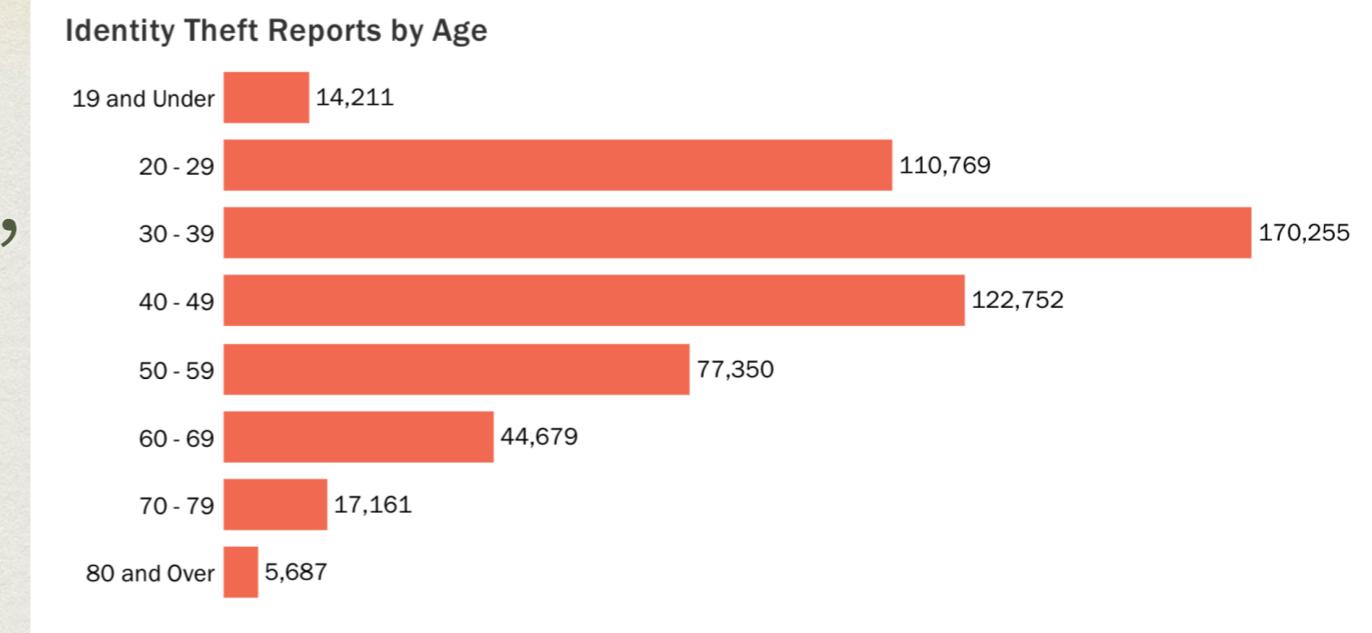
UN GRAND CLASSIQUE

Identity Theft Reports by Type

Theft Type	Theft Subtype	# of Reports	% Difference from Previous Year
Credit Card Fraud	New Accounts	246,763	+88%
	Existing Accounts	31,022	-4%
Loan or Lease Fraud	Apartment or House Rented	8,508	+56%
	Auto Loan\Lease	38,561	+105%
	Business\Personal Loan	43,919	+116%
	Federal Student Loan	14,633	+188%
	Non-Federal Student Loan	11,025	+74%
	Real Estate Loan	7,706	+49%
Phone or Utilities Fraud	Landline Telephone – Existing Accounts	1,737	+20%
	Landline Telephone – New Accounts	10,854	+40%
	Mobile Telephone – Existing Accounts	5,630	+13%
	Mobile Telephone – New Accounts	44,208	+32%
	Utilities – Existing Accounts	1,449	+9%
	Utilities – New Accounts	29,591	+34%
Bank Fraud	Debit Cards, Electronic Funds Transfer, or ACH	23,226	+0%
	Existing Accounts	12,520	-4%
	New Accounts	27,129	+38%
Employment or Tax-Related Fraud	Employment or Wage-Related Fraud	19,835	-35%
	Tax Fraud	27,454	-29%
Government Documents or Benefits Fraud	Driver's License Issued\Forged	5,007	+11%
	Government Benefits Applied For\Received	12,896	-20%
	Other Government Documents Issued\Forged	6,710	+19%
	Passport Issued\Forged	757	+8%

CIBLES PRIVILÉGIÉES

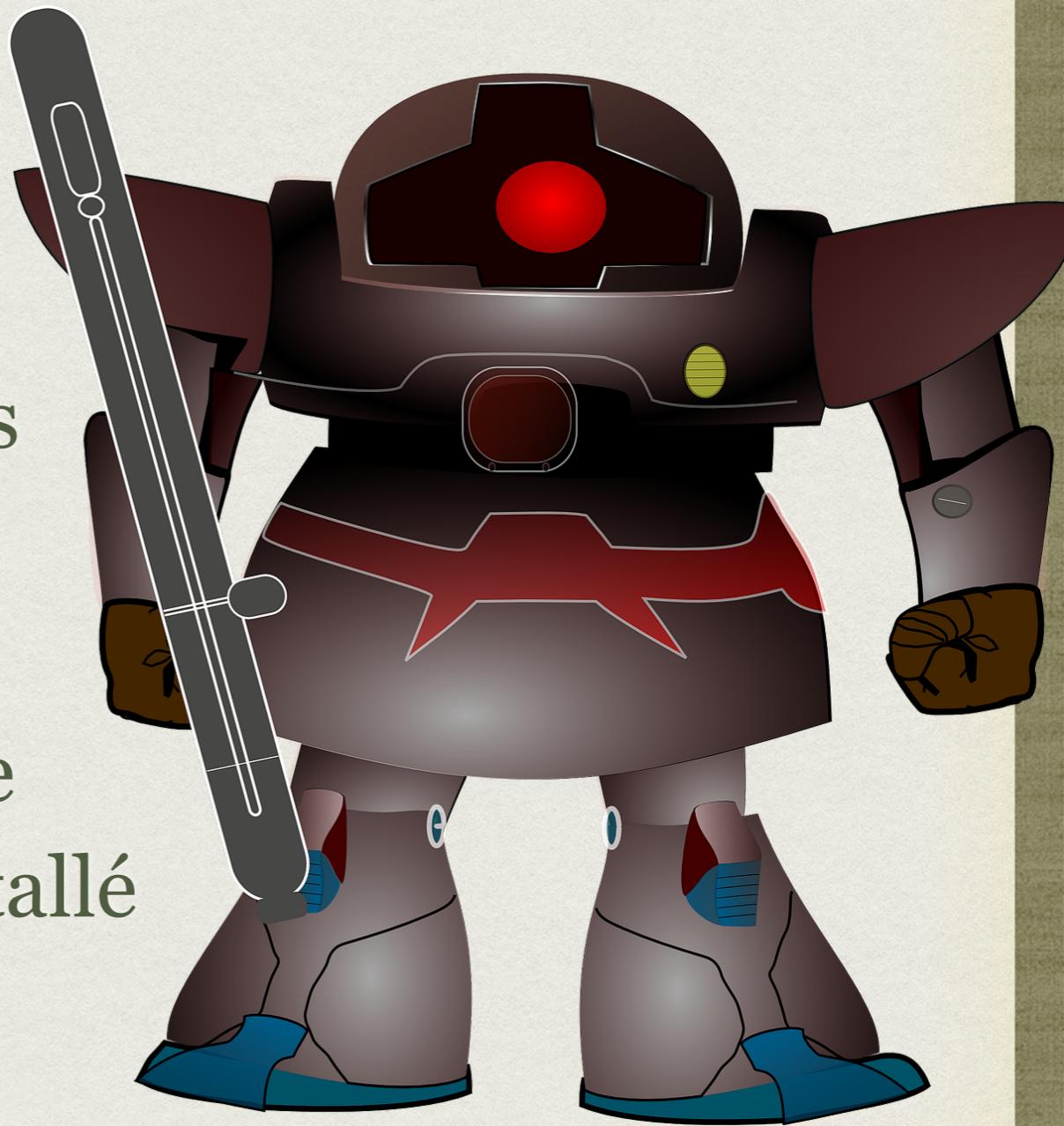
- Jeunes (plus connectés, réseaux sociaux)
- Vieux (plus crédules)
- Militaires (plus de social)
- Morts (ne se plaignent pas)



BOTNETS

C'EST QUOI ?

- réseau de machines sous le contrôle d'un adversaire
- utilisées pour monter d'autres attaques
- chaque machine a été infectée préalablement, un troyen installé et mis à jour régulièrement



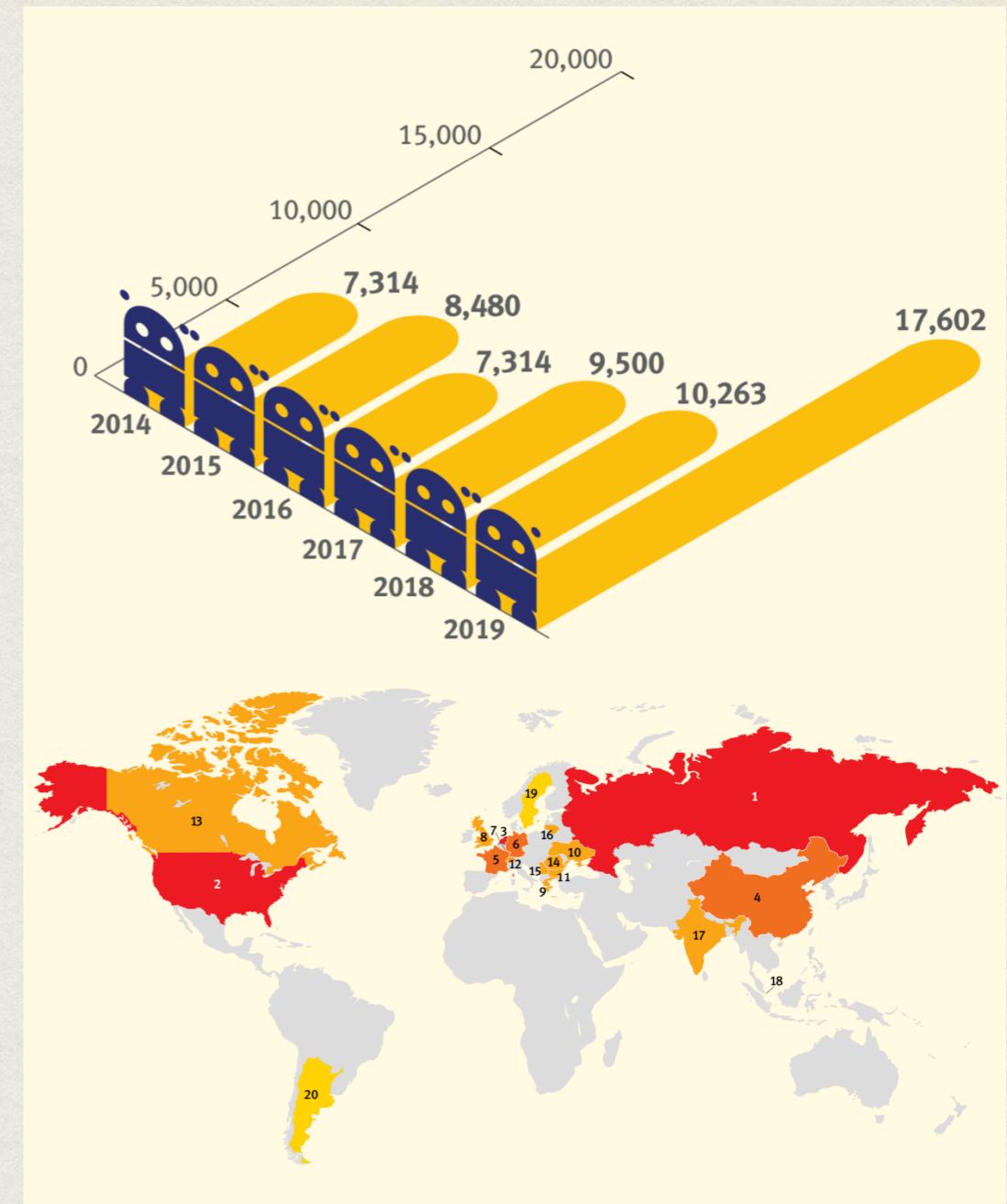
WHAT?

- **dizaines millions** de PCs (et d'objets connectés) dans le monde **sont contrôlés** par des « pirates » à l'insu de leurs propriétaires légitimes, are you kidding me ?



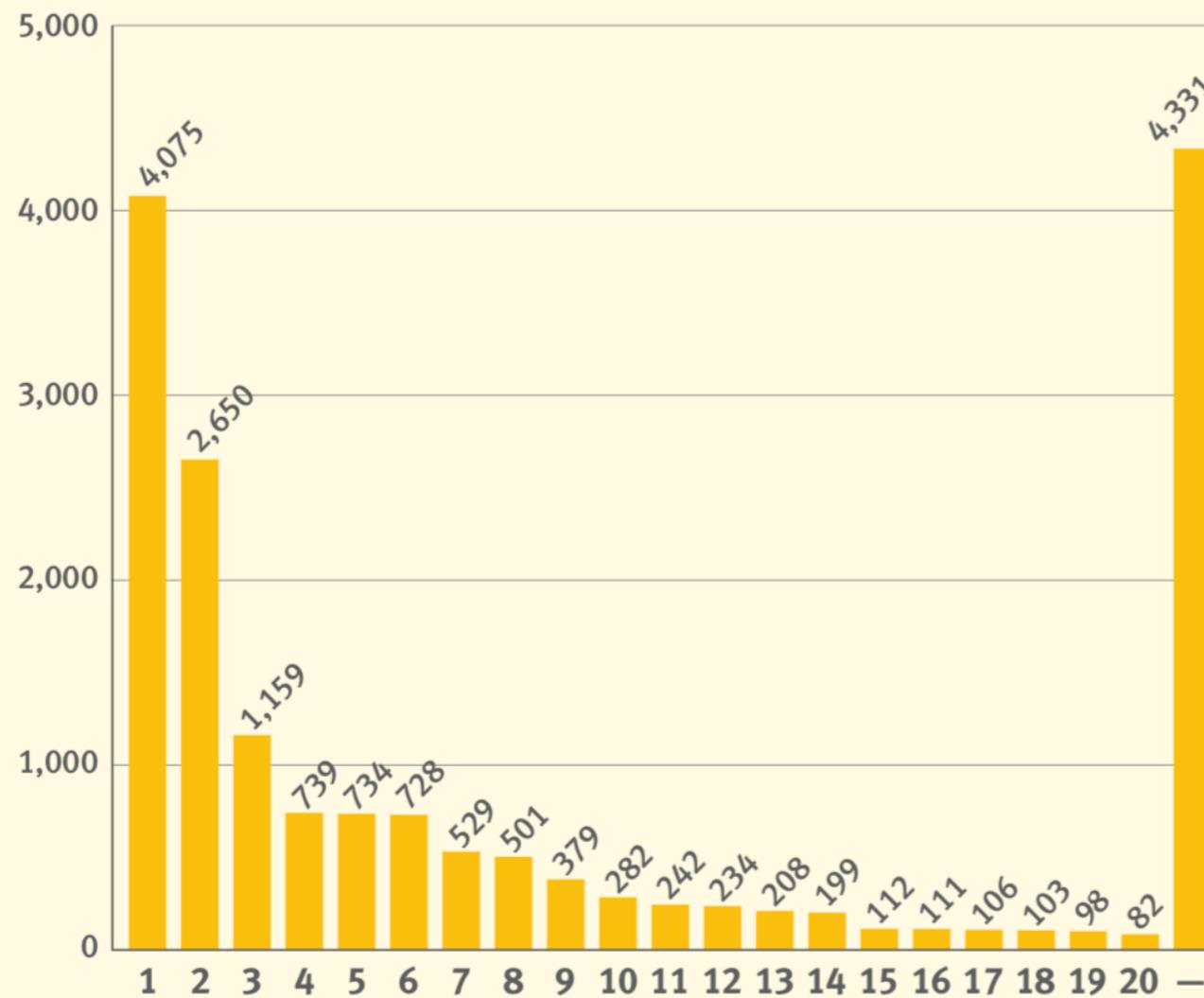
FAITS

- +17000 C&C en 2019 de tailles diverses :
 - 2016 Miraï était estimé entre 800k et 2.5M de noeuds
 - 2018 Hajime 300k noeuds IOT (en 2020 ~20B noeud IOT à la sécurité ... précaire, cf. shodan.io)
 - 2019 Emotet un des plus actifs actuellement a été mesuré a ~120k @IP uniques
- répartis de par le monde: 1-Russie, 2-USA, 3-Pays-bas, ..., 13-Canada



DIFFÉRENTES FAMILLES DE MALWARE

Malware families associated with 2019 botnet C&C listings



Rank	Malware	Note	% change
1	Lokibot	Credential Stealer	+74%
2	AZORult	Credential Stealer	+190%
3	NanoCore	Remote Access Tool (RAT)	+181%
4	Pony	Dropper/Credential Stealer	-23%
5	TrickBot	e-banking trojan	+173%
6	Gozi	e-banking trojan	+76%
7	Emotet	Dropper/Backdoor	-23%
8	RemocsRAT	Remote Access Tool (RAT)	+147%
9	Predator Stealer	Credential Stealer	—
10	Adwind/JBifrost	Remote Access Tool (RAT)	-78%
11	NetWire	Remote Access Tool (RAT)	+98%
12	KPOTStealer	Credential Stealer	—
13	ArkeiStealer	Credential Stealer	+197%
14	NjRAT	Remote Access Tool (RAT)	+290%
15	AgentTesla	KeyLogger/Credential Stealer	-4%
16	QuasarRAT	Remote Access Tool (RAT)	—
17	Dridex	e-banking trojan	—
18	HawkEye	Credential Stealer	—
19	IcedID	e-banking trojan	—
20	CoinMiner	Various crypto currency miners	-8%
—	Others	Other malware families	—

CHARGES ?

- Passif - Spyware, voleurs de credentials (60%): récupèrent les login/password, #credit, comptes bancaires, etc. de l'hôte
- Actif - Campagnes de spam, relais d'infection, installation d'autres malware sur l'hôte, installation ou relais de ransomware
- I/O - Remote Access Tools (RATs) (19%): permettent le contrôle complet à distance de l'hôte

DDOS

DÉNI DE SERVICE DISTRIBUÉ (DISTRIBUTED DENIAL OF SERVICE)

- de façon **coordonnée**, différents noeuds submergent de requêtes un serveur, le faisant s'écrouler
- **motivations** : politiques, vengeance d'un ex-employé, hacktivistes, chantage du crime organisé, compétition entre entreprises, etc.
- Q1-2020 : **+500%** / Q4-2019
 - taille max **176Gbps**
 - 50% de Chine ; 13% USA ; 9% Russie

TECHNIQUEMENT

- A partir d'un botnet
- **UDP** (75%): on submerge directement de paquets UDP, sert parfois d'écran de fumée pour **camoufler** une autre attaque
- **DNS Amplification** (10%): on utilise de grandes requêtes DNS avec une @IP falsifiée (spoofed), les serveurs DNS servent de relais à leur insu
- **CLDAP** (5%) : idem mais serveur LDAP
- Autres: TCP Ack, TCP Syn, application, amplification, etc.

RANÇONGICIELS

A T'ON BESOIN D'EXPLIQUER CE QUE C'EST ?

- Malware qui **chiffre** vos données et demande une **rançon**
 - ANSSI : +100% en France entre septembre 2020 / 2019
 - Vulnérabilités accrues dues au BYOD en sortie de confinement
 - De nombreuses villes/services publics/hôpitaux sont touchés (sécurité faible, service essentiel, forte incitation à payer la rançon)
- En **prévention**: résister aux hameçonnages, antivirus, IDS, systèmes à jour, etc.
- En **réparation**: existe t'il un backup non contaminé ? To pay or **not to pay** ? Assurances

PAYER OU PAS ?

- **Payer ?**
 - On récupère ses données (**ou pas**)
 - On n'est pas à l'abri que cela recommence (en 2018 **50% des victimes étaient attaquées plusieurs fois** - source Sophos)
 - On encourage le système
- **Ne pas payer** (recommandé par les agences) ?
 - On ne récupère pas ses données, notre « business » est bloqué
 - On risque une divulgation de ses données potentiellement critiques
 - On n'encourage pas le système

EXEMPLE DE BALTIMORE

- 7 Mai 2019: le virus RobbinHood neutralise 10000 postes Windows de la ville de Baltimore, Maryland
- Rançon demandée : 100.000 USD en btc
- 28 Mai le FBI interdit le paiement de la rançon
- le code de RobbinHood est partiellement issu de EternalBlue, un **outil offensif développé par la NSA** (siège au Maryland) et volé par le groupe ShadowHackers en 2017 et depuis utilisé par des hackers d'état Nord Coréen, Russes et Chinois
- Il existe un patch Microsoft contre EternalBlue depuis 2017 mais **la ville n'a pas fait de mise à jour entre 2017 et 2019** ...
- Pas de paiement d'impôts en lignes, pas d'amendes de stationnement, pas de caméra de surveillance, pas de factures d'eau (compteurs intelligents), données personnelles et de paiement fuitées
- Cout : $\sim 40M\$ = 18 M\$$ (10M\$ système info., 1M\$ rachat postes info., 8M\$ perte de revenu) + 22M\$ perte des données

AUTRES EXEMPLES

- **WannaCry** (2017) : **EternalBlue** ~200000 infections, de l'ordre du milliard \$US, attribué à la Corée du Nord
- **ISS World** (fev2020) : 1 mois d'interruption de service et ~100M\$ de frais de recouvrement/mitigation
- **Garmin** (juill2020) : *WastedLocker*, rançongiciel ciblé : chiffrement priorisé, chiffrement de ressources réseau, etc. rançon demandée **10M\$** par *Evil Corp*, dommage à l'image ?

AP

German Hospital Hacked, Patient Taken to Another City Dies

By Associated Press on September 17, 2020

[Share](#)[Tweet](#)[Recommender 0](#)[RSS](#)

German authorities said Thursday that what appears to have been a misdirected hacker attack caused the failure of IT systems at a major hospital in Duesseldorf, and a woman who needed urgent admission died after she had to be taken to another city for treatment.

The Duesseldorf University Clinic's systems have been disrupted since last Thursday. The hospital said investigators have found that the source of the problem was a hacker attack on a weak spot in "widely used commercial add-on software," which it didn't identify.

As a consequence, systems gradually crashed and the hospital wasn't able to access data; emergency patients were taken elsewhere and operations postponed.

The hospital said that that "there was no concrete ransom demand." It added that there are no indications that data is irretrievably lost and that its IT systems are being gradually restarted.

A report from North Rhine-Westphalia state's justice minister said that 30 servers at the hospital were encrypted last week and an extortion note left on one of the servers, news agency dpa reported. The note — which called on the addressees to get in touch, but didn't name any sum — was addressed to the Heinrich Heine University, to which the Duesseldorf hospital is affiliated, and not to the hospital itself.

Duesseldorf police then established contact and told the perpetrators that the hospital, and not the university, had been affected, endangering patients. The perpetrators then withdrew the extortion attempt and provided a digital key to decrypt the data. The perpetrators are no longer reachable, according to the justice minister's report.

Prosecutors launched an investigation against the unknown perpetrators on suspicion of negligent manslaughter because a patient in a life-threatening condition who was supposed to be taken to the hospital last Friday night was sent instead to a hospital in Wuppertal, a roughly 32-kilometer (20-mile) drive. Doctors weren't able to start treating her for an hour and she died.



Bart Preneel @bpreneel1

19m

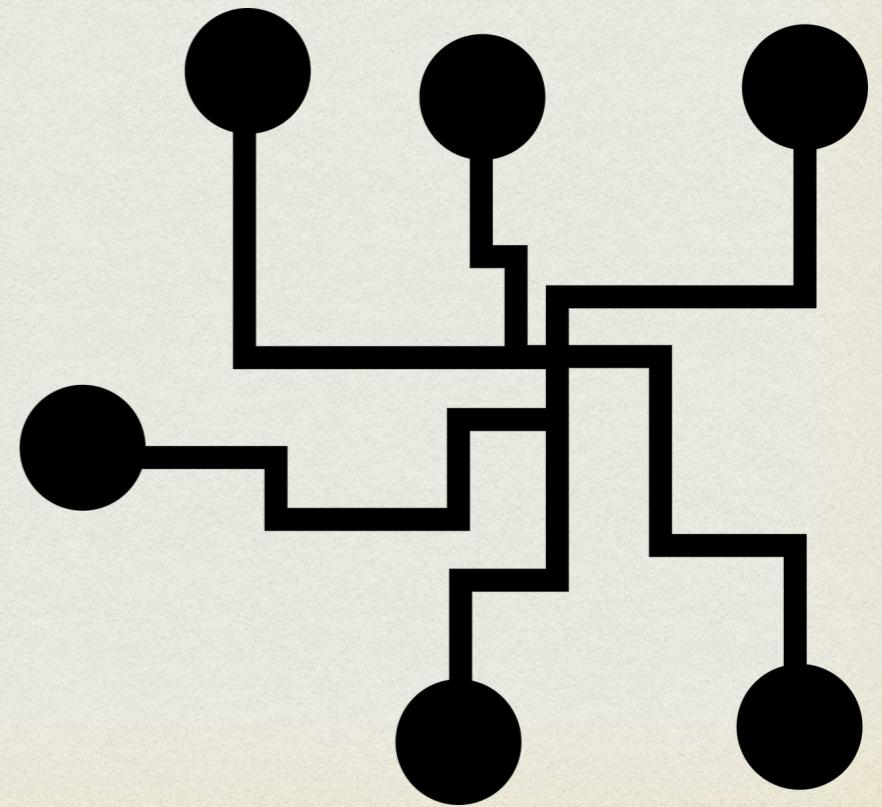
Many times predicted in security talks. Now a sad reality. German Hospital Hacked, Patient Taken to Another City Dies

[securityweek.com/german-hospital...](http://securityweek.com/german-hospital-hacked-patient-taken-to-another-city-dies)
via @SecurityWeek

ECONOMIE DE LA SÉCURITÉ

DES ACTEURS VARIÉS

- **Etats** avec des postures différentes (offensives/défensives)
 - enjeux géopolitiques, politiques, intelligence, militaires et économiques
 - ex. Chine, Corée du Nord, USA, Russie, France
 - agences étatiques : NSA, ANSSI, etc.
- **Criminels**, organisés ou semi-organisés ou indépendants
 - APT41, Evil Corp, équipes *adhoc* issues d'un forum, etc.
- **Entreprises**, proies ou de sécurité (off/def/prev) ; assurances
- **Individus**, proies ou acteurs ; scientifiques; hackers; etc.
- Plein de liens divers et variés entre ces acteurs !





- Protéger son/ses entreprises contre les attaques (DDOS, vols de tech., etc.)
- Protéger ses infrastructures, son système démocratique, sa Société
- Préparer **l'offensive** pour mieux se défendre ...
- autres motifs mais ...



Couts

Bénéfices



- Influence (politique)
- Intelligence (économique, technologique)



- Influence (politique)
- Intelligence (économique, technologique)



ÉVOLUTION VERS LE CYBERCRIME

- C'est plus une **économie** qu'un **business** qui reprend les clés du capitalisme contemporain
 - Startups, info-nuagique, supermarchés d'outils à la Amazon
 - Des monnaies numériques « spécialisées »
 - Des agents spécialisés: producteurs, fournisseurs, vendeurs, consommateurs de différents biens
- Les biens échangés sont divers et variés
 - Numéros de carte de crédit, « likes », points de cartes de fidélité, login/passwords, recettes de soda et autres secrets d'affaire, données personnelles, outils technologiques d'état
 - Des spécialisations géographiques avec des pays exportateurs et des pays importateurs
 - Professionnalisation grandissante : centres de formation, consultants en CV, recommandations personnelles références

CYBERCRIME

- Un « marché » de **1500 Milliards** de US\$ en 2018

Crime	Annual Revenues*
Illicit, illegal online markets	\$860 billion
Trade secret, IP theft	\$500 billion
Data trading**	\$160 billion
Crimeware, CaaS (Cybercrime-as-a-Service)	\$1.6 billion
Ransomware***	\$1 billion

*totals are approximate

**Revenues derived from trading in stolen data, such as: credit and debit card information banking log-in details, loyalty schemes and so on

***Revenues derived from extortions based on encrypting data and demanding payments

Table 1: Annual Cybercrime Revenue Estimates

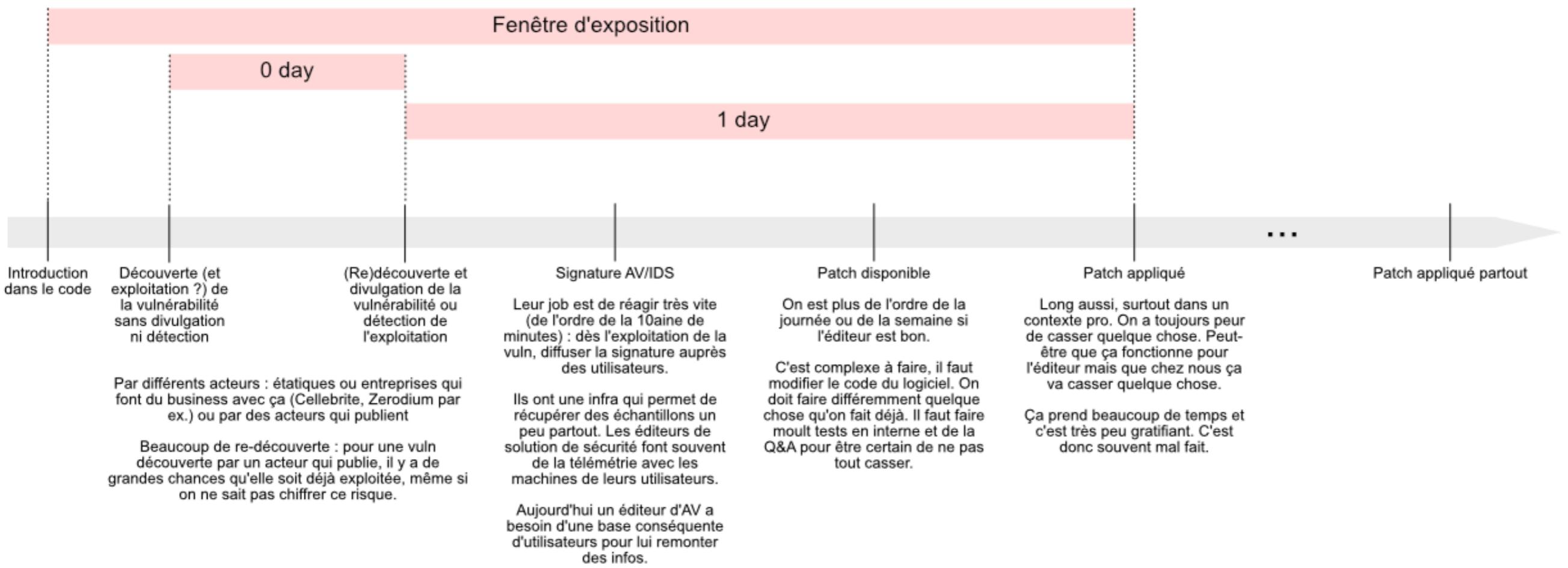
Source: Bromium - Into the Web of Profit

VULNÉRABILITÉS JOUR-ZÉRO (o-DAY)

- Une vulnérabilité qui n'a pas encore été publiée
 - et donc contre laquelle il n'existe pas de correctif
- Dans le jeu du chat et de la souris entre attaquants et protecteurs, la « o-day » constitue un **avantage temporel** important et offre a priori une **grande surface d'attaque**
- On les considère aujourd'hui comme de potentielles *armes de destruction massive*
 - Les o-day détenues (trouvées ou achetées) par les agences fédérales US sont évaluées pour savoir si elles sont révélées ou conservées secrètes pour exploitation
 - ex: CVE-2020-0601 faille dans Crypt32.dll de Win10, WinServer16 et 19, révélée par la NSA puis patchée en janvier 2020.
 - **Questions** : quand ont ils trouvé cette faille, étaient ils les seuls à la connaître, que se passe t'il pour ceux qui traînent à patcher leur Windows, etc...

VULNÉRABILITÉS JOUR-ZÉRO (o-DAY)

Cycle de vie des vulnérabilités



MARCHÉ DES FAILLES

« O-DAY »

ZERODIUM Payouts for Desktops/Servers*											
Up to \$1,000,000											
Up to \$500,000											
Up to \$250,000											
Up to \$200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux			4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.001 Apache RCE Linux	2.002 MS IIS RCE Win	1.001 Win RCE Zero Click Win
Up to \$100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux		
Up to \$80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win		
Up to \$50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD		
Up to \$10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux		

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

MARCHÉ DES FAILLES

« O-DAY »

	ZERODIUM Payouts for Mobiles*									
Up to \$2,500,000										
Up to \$2,000,000										
Up to \$1,500,000										
Up to \$1,000,000										
Up to \$500,000	3.001 Persistence IOS	2.005 WeChat RCE+LPE IOS/Android	2.006 iMessage RCE+LPE IOS	2.007 FB Messenger RCE+LPE IOS/Android	2.008 Signal RCE+LPE IOS/Android	2.009 Telegram RCE+LPE IOS/Android	2.010 Email App RCE+LPE IOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE IOS	
Up to \$200,000	5.001 Baseband RCE+LPE IOS/Android		6.001 LPE to Kernel/Root IOS/Android	2.011 Media Files RCE+LPE IOS/Android	2.012 Documents RCE+LPE IOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari IOS	4.006 Safari RCE w/o SBX IOS	
Up to \$100,000	7.001 Code Signing Bypass IOS/Android	5.002 WiFi RCE IOS/Android	5.003 RCE via MitM IOS/Android	6.002 LPE to System Android	8.001 Information Disclosure IOS/Android	8.002 [k]ASLR Bypass IOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass IOS	9.003 Touch ID Bypass IOS	

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

RAPPELS ARITHMÉTIQUES

Pour la cryptographie

ALGÈBRE DE BOOLE

- En binaire, on considère des mots $\{0,1\}^n$
- Les opérateurs communs sont :
 - $a \wedge b = c$
 - $a \vee b = c$
 - $\neg a = b$
 - $a \oplus b = c$

ALGÈBRE DE BOOLE

- En binaire, on considère des mots $\{0,1\}^n$
- Les opérateurs communs sont :
 - $a \wedge b = c$
 - $a \vee b = c$
 - $\neg a = b$
 - $a \oplus b = c$

C	O	1
O	O	O
1	O	1

ALGÈBRE DE BOOLE

- En binaire, on considère des mots $\{0,1\}^n$
- Les opérateurs communs sont :
 - $a \wedge b = c$
 - $a \vee b = c$
 - $\neg a = b$
 - $a \oplus b = c$

C	O	1
0	0	1
1	1	1

ALGÈBRE DE BOOLE

- En binaire, on considère des mots $\{0,1\}^n$
- Les opérateurs communs sont :
 - $a \wedge b = c$
 - $a \vee b = c$
 - $\neg a = b$
 - $a \oplus b = c$

A	O	1
B	1	O

ALGÈBRE DE BOOLE

- En binaire, on considère des mots $\{0,1\}^n$
- Les opérateurs communs sont :
 - $a \wedge b = c$
 - $a \vee b = c$
 - $\neg a = b$
 - $a \oplus b = c$

C	O	1
O	O	1
1	1	O

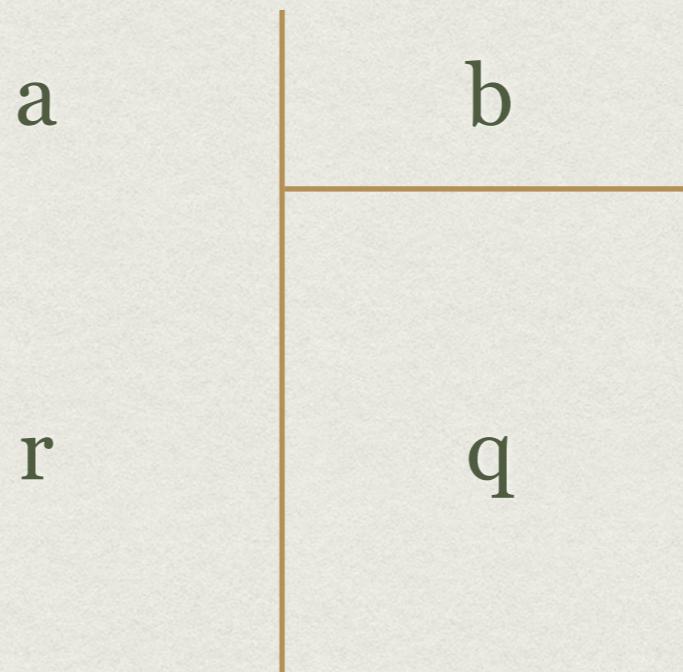
DIVISION EUCLIDIENNE

- Soit $a \in \mathbb{Z}, b \in \mathbb{N}^*$, il existe $q, r \in \mathbb{Z}$ uniques t.q.
 $a = b \cdot q + r$ et $0 \leq r < b$



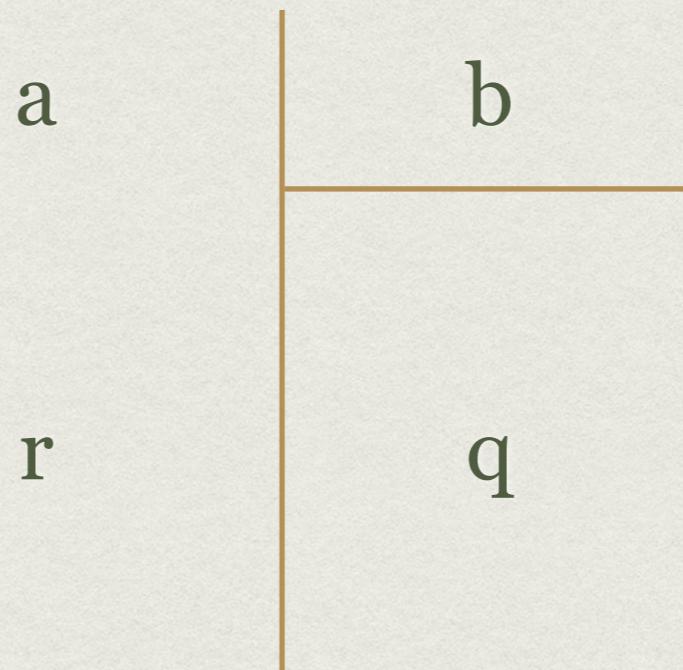
DIVISION EUCLIDIENNE

- Soit $a \in \mathbb{Z}, b \in \mathbb{N}^*$, il existe $q, r \in \mathbb{Z}$ uniques t.q.
 $a = b \cdot q + r$ et $0 \leq r < b$



DIVISION EUCLIDIENNE

- Soit $a \in \mathbb{Z}, b \in \mathbb{N}^*$, il existe $q, r \in \mathbb{Z}$ uniques t.q.
 $a = b \cdot q + r$ et $0 \leq r < b$



- Si $r=0$ alors b divise a : $b|a$

DIVISION EUCLIDIENNE

- Soit $a \in \mathbb{Z}, b \in \mathbb{N}^*$, il existe $q, r \in \mathbb{Z}$ uniques t.q.
 $a = b \cdot q + r$ et $0 \leq r < b$
- Plus grand diviseur commun : PGCD(a,b)
- Algorithme d'Euclide pour la division : $a = b \cdot q + r$
- Lemme : $\text{pgcd}(a,b) = \text{pgcd}(b,r)$

ALGO D'EUCLIDE

- On veut calculer le $\text{pgcd}(600, 124)$

ALGO D'EUCLIDE

- On veut calculer le $\text{pgcd}(600,124) = \text{pgcd}(b,r)$
- $600 = 124 \cdot 4 + 104$

ALGO D'EUCLIDE

- On veut calculer le $\text{pgcd}(600, 124) = \text{pgcd}(124, 104)$
- $600 = 124 \cdot 4 + 104$
- $124 = 104 \cdot 1 + 20$
-

ALGO D'EUCLIDE

- On veut calculer le $\text{pgcd}(600, 124) = \text{pgcd}(104, 20)$
- $600 = 124 \cdot 4 + 104$
- $124 = 104 \cdot 1 + 20$
- $104 = 20 \cdot 5 + 4$
-

ALGO D'EUCLIDE

- On veut calculer le $\text{pgcd}(600,124) = \text{pgcd}(104,20)$
- $600 = 124 \cdot 4 + 104$
- $124 = 104 \cdot 1 + 20$
- $104 = 20 \cdot 5 + 4$
- $20 = 4 \cdot 5 + 0$

ALGO D'EUCLIDE

- On veut calculer le $\text{pgcd}(600,124) = \text{pgcd}(104,20) = 4$
- $600 = 124 \cdot 4 + 104$
- $124 = 104 \cdot 1 + 20$
- $104 = 20 \cdot 5 + 4$
- $20 = 4 \cdot 5 + 0$

NOMBRES PREMIERS ENTRE EUX

- Deux nombres a, b sont premiers entre eux si $\text{PGCD}(a,b)=1$

THÉORÈME DE BÉZOUT

- Soit a, b entiers,
 $\exists u, v \in \mathbb{Z} : a \cdot u + b \cdot v = PGCD(a, b)$
- u, v : les coefficients de Bézout
- Ils sont obtenus en *remontant* l'algo d'Euclide

ALGO D'EUCLIDE

- On cherche u, v tq $600.u + 124.v = 4$
- $600 = 124 \cdot 4 + 104$
- $124 = 104 \cdot 1 + 20$
- $104 = 20 \cdot 5 + 4$
- $20 = 4 \cdot 5 + 0$

ALGO D'EUCLIDE

- On cherche u, v tq $600.u + 124.v = 4$
- $600 = 124 \cdot 4 + 104$
- $124 = 104 \cdot 1 + 20$
- $104 = 20 \cdot 5 + 4$ $4=104-20.5$
- $20 = 4 \cdot 5 + 0$

ALGO D'EUCLIDE

- On cherche u, v tq $600.u + 124.v = 4$
- $600 = 124 \cdot 4 + 104$
- $124 = 104 \cdot 1 + 20$ $4 = 104 - (124 - 104 \cdot 1) \cdot 5$
- $104 = 20 \cdot 5 + 4$ $4 = 104 - 20 \cdot 5$
- $20 = 4 \cdot 5 + 0$

ALGO D'EUCLIDE

- On cherche u, v tq $600.u + 124.v = 4$
- $600 = 124 \cdot 4 + 104$
- $124 = 104 \cdot 1 + 20$ $4 = 124 \cdot (-5) + 104 \cdot 6$
- $104 = 20 \cdot 5 + 4$ $4 = 104 - 20 \cdot 5$
- $20 = 4 \cdot 5 + 0$

ALGO D'EUCLIDE

- On cherche u, v tq $600.u + 124.v = 4$
- $600 = 124 \cdot 4 + 104$ $4 = 124 \cdot (-5) + (600 - 124 \cdot 4) \cdot 6$
- $124 = 104 \cdot 1 + 20$ $4 = 124 \cdot (-5) + 104 \cdot 6$
- $104 = 20 \cdot 5 + 4$ $4 = 104 - 20 \cdot 5$
- $20 = 4 \cdot 5 + 0$

ALGO D'EUCLIDE

- On cherche u, v tq $600.u + 124.v = 4$
- $600 = 124 \cdot 4 + 104$ $4 = 600 \cdot 6 + 124 \cdot (-29)$
- $124 = 104 \cdot 1 + 20$ $4 = 124 \cdot (-5) + 104 \cdot 6$
- $104 = 20 \cdot 5 + 4$ $4 = 104 - 20 \cdot 5$
- $20 = 4 \cdot 5 + 0$

ALGO D'EUCLIDE

- On cherche u, v tq $600.u + 124.v = 4$
- $600 = 124 \cdot 4 + 104$ $u=6, v=-29$
- $124 = 104 \cdot 1 + 20$
- $104 = 20 \cdot 5 + 4$
- $20 = 4 \cdot 5 + 0$

ALGO D'EUCLIDE

- On cherche u, v tq $600.u + 124.v = 4$
- $600 = 124 \cdot 4 + 104$ $u=6, v=-29$
- $124 = 104 \cdot 1 + 20$ $600.6+124.(-29)=?$
- $104 = 20 \cdot 5 + 4$
- $20 = 4 \cdot 5 + 0$

ALGO D'EUCLIDE

- Autre exemple : $a=9945$ $b=3003$
 - Calculer $\text{PGCD}(a,b)$
 - Calculer u,v tq $a.u+b.v = \text{PGCD}(a,b)$

NOMBRES PREMIERS

- Un nombre premier p est un entier ≥ 2 dont les seuls diviseurs sont 1 et p
- 2,3,5,7,11,13,17,19,23,27,29,31....
- On peut décomposer un nombre en facteurs premiers
 - $600 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdot 17^0 \cdot 19^0 \cdot 23^0 \cdot 27^0 \cdot 29^0 \cdot 31^0$
 - $124 = 2^2 \cdot 31^1$
- Pour le PGCD, plus petits exposants :
$$PGCD(600,124) = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdot 17^0 \cdot 19^0 \cdot 23^0 \cdot 27^0 \cdot 29^0 \cdot 31^0 = 4$$
- Pour le PPCM, plus grands exposants : $PPCM(600,124) = 2^3 \cdot 3^1 \cdot 5^2 \cdot 31^1 = 18600$