Revue d'actualité de l'OSSIR

13 septembre 2022

Christophe Chasseboeuf
*Vladimir Kolla @mynameisv_*

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Outlook, CVE-2022-35742

- Déni de service à la réception d’un mail

```
--A
Content-Type:aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Content-Type:application

--A--
```

https://github.com/78ResearchLab/PoC/tree/main/CVE-2022-35742

NTFS, CVE-2021-31956

- Elévation de privilèges (exécution de code)
- Découvert exploité dans la nature

https://research.nccgroup.com/2021/07/15/cve-2021-31956-exploiting-the-windows-kernel-ntfs-with-wnf-part-1/

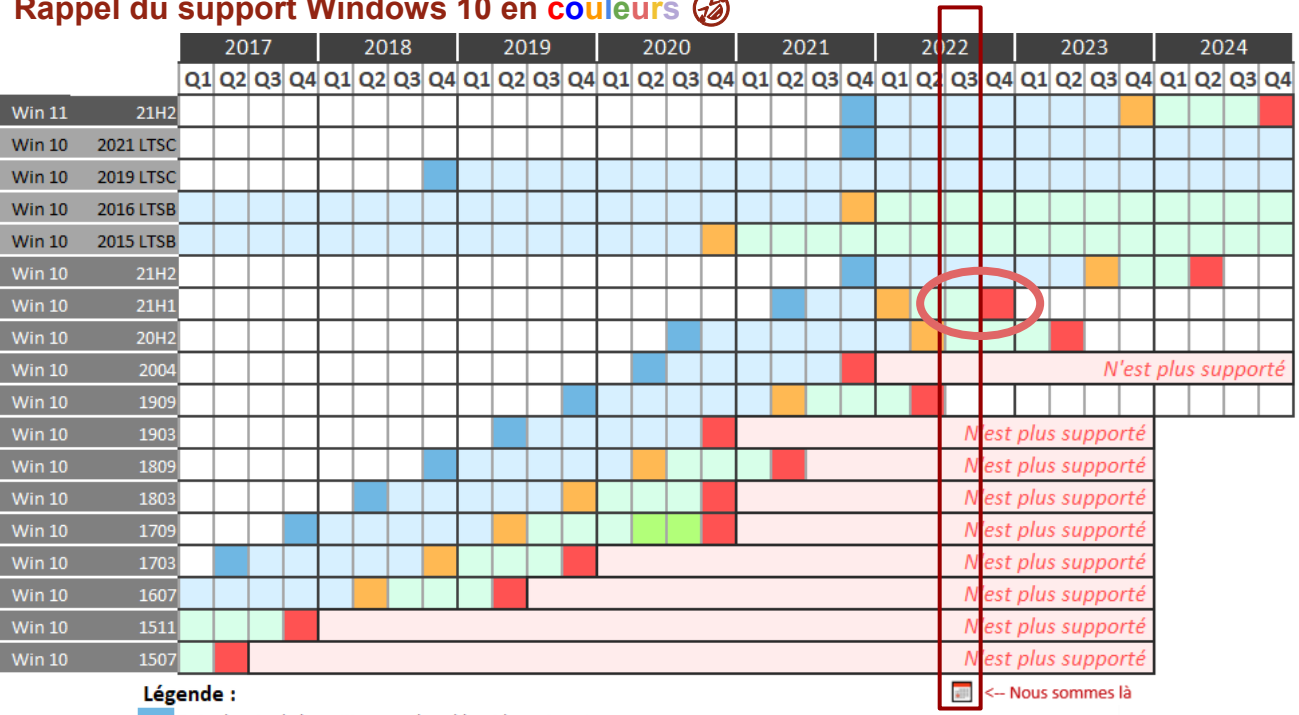
NFS v4, CVE-2022-30136

- Elévation de privilèges (exécution de code)

https://www.coresecurity.com/core-labs/articles/analysis-cve-2022-30136-windows-network-file-system-vulnerability

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs



Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour les versions Home, Pro, Pro or Workstations / fin de support standard pour LTSB/LTSC
- Support uniquement pour les versions Enterprise et Education
- Prolongation exceptionnelle suite au Coronavirus
- Fin de support pour toutes les versions / fin de support étendu pour LTSB/LTSC

Sortie	Home, Pro	Entreprise
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	?
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029
mardi 2 août 2016	mardi 12 octobre 2021	mardi 13 octobre 2026
mercredi 29 juillet 2015	mardi 13 octobre 2020	mardi 14 octobre 2025
mardi 16 novembre 2021	jeudi 13 juillet 2023	mardi 11 juin 2024
mardi 18 mai 2021	mardi 13 décembre 2022	mardi 13 décembre 2022
mardi 20 octobre 2020	mardi 10 mai 2022	mardi 9 mai 2023
mercredi 27 mai 2020	mardi 14 décembre 2021	mardi 14 décembre 2021
mardi 12 novembre 2019	mardi 11 mai 2021	10 mai 2022••
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	11 mai 2021••
lundi 30 avril 2018	mardi 12 novembre 2019	mardi 10 novembre 2020
mardi 17 octobre 2017	~~9 avril~~ 4 sept. 2019	~~14 avril~~ 13 oct. 2020
5 avril 2017•	mardi 9 octobre 2018	mardi 8 octobre 2019
mardi 2 août 2016	mardi 10 avril 2018	mardi 9 avril 2019
mardi 10 novembre 2015	mardi 10 octobre 2017	mardi 10 octobre 2017
mercredi 29 juillet 2015	9 mai 2017	mardi 9 mai 2017

Failles / Bulletins / Advisories
Microsoft - Divers

Les macros Office, la suite de l'ascenseur émotionnel

- ✌ Février 2022 : Annonce de la désactivation des macros https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/bc-p/3566717
- 🎉 Avril 2022 : macros désactivées pour les fichiers venant d'internet https://www.ossir.org/paris/supports/2022/2022-02-08/2022-02-08_OSSIR-20220208-v0.1.pdf
- 😢 Juin 2022 : retour en arrière sans explication, à priori suite à des plaintes d'utilisateurs https://www.bleepingcomputer.com/news/microsoft/microsoft-rolls-back-decision-to-block-office-macros-by-default/
- 🤡 Juillet 2022 : en fait… si, peut-être un déactivation, prochainement : https://www.theverge.com/2022/7/11/23203554/microsoft-block-office-vba-macros-changes-temporary-statement
- 🤧 Juillet 2022 : désactivation mais avec une réactivation à la main des clients : https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/bc-p/3566717

Les macros Office sont désactivées ?

- Et les exécutions de code DDE ?

  https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

GLibC fuite de mémoire (CVE-2022-39046)

- Une vulnérabilité dans GLibC 😳😱😱😱😱😱
  - Ecriture de la mémoire dans le fichier de log si Syslog reçoit un message > 1024 octets
  - Complexe de récupérer les résultats
  - Exploit : https://sourceware.org/bugzilla/show_bug.cgi?id=29536

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39046

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Apache 2.4, vulnérabilité présente depuis 20 ans

- Lecture et écriture arbitraire de mémoire
  - https://www.openwall.com/lists/oss-security/2022/08/09/2
- Décrite dans 'The Art of Software Security Assessment'
  - Livre publié en 2006 et vuln jamais corrigée

Listing 8-6. If Header Processing Vulnerability in Apache's mod_dav Module

```
while (*list) {
  /* List is the entire production (in a URI scope) */
switch (*list) {
```

420

The Art of Software Security Assessment - Identifying and Preventing Software Vulnerabilities

```
case 'N':
  if (list[1] == 'o' && list[2] == 't') {
    if (condition != DAV_IF_COND_NORMAL) {
      return dav_new_error(r->pool, HTTP_BAD_REQUEST,
                           DAV_ERR_IF_MULTIPLE_NOT,
                           "Invalid \"If:\" header: "
                           "Multiple \"not\" entries "
                           "for the same state.");
    }
    condition = DAV_IF_COND_NOT;
  }
  list += 2;
  break;
```

This code fails to check for NUL terminators correctly when it encounters an `N` character. The `N` case should check for the presence of the word "`Not`" and then skip over it. However, the code skips over the next two characters anytime it encounters an `N` character. An attacker can specify a header string ending with an `N` character, meaning an `N` character followed by a NUL character. Processing will continue past the NUL character to data in memory adjacent to the string being parsed. The vulnerable code path is demonstrated by the bolded lines in the listing.

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Tu rentres ou tu ne rentres pas dans mon réseau à travers les API ??

- Rapport sur l'état de l'API (2022) de Postman *(plateforme d'hébergement d'API)*
- Trouvailles clés
  - 1) Les développeurs passent la plupart de leur temps sur les APIs
  - 2) Les investissements dans les API resteront importants, malgré les vents contraires de l'économie.
  - 3) Les leaders de l'API sont plus performants
  - 4) Le travail à distance est "très important".
  - 5) L'intégration des API internes est primordiale
  - **6) Le manque de compétences en matière de conception d'API est un problème majeur**

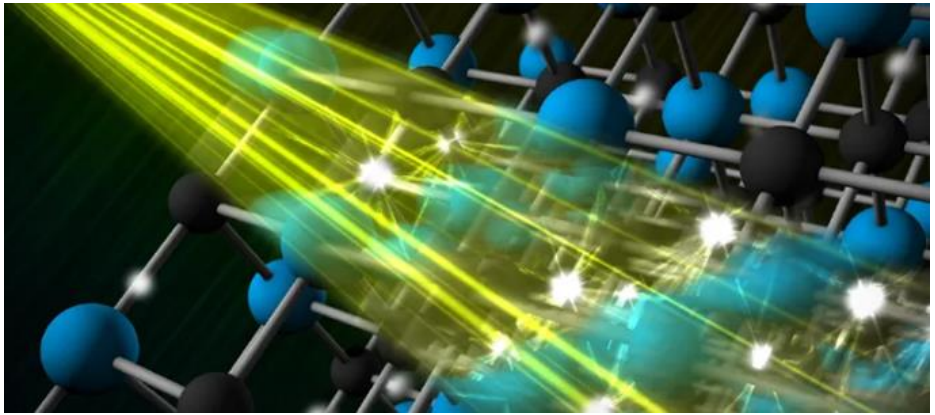
https://www.postman.com/state-of-api/

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Conférence Black Hat sur Electron

- Exploitation d'Electron (Chromium + javascript multiplateforme Node JS)
- Exécution de code à distance dans des applications comme Discord, Teams (lecture de fichiers locaux), VSCode, Basecamp, Mattermost, Element, Notion, Slack et d'autres.

https://www.vice.com/en/article/m7gb7y/researchers-find-vulnerability-in-software-underlying-discord-microsoft-teams-and-other-apps



Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Zoom sur macOS, élévation locale de privilèges (CVE-2022-28751 et CVE-2022-28756)

- Présenté à DefCon comme une 0-day
  - Appels XPC pour lancer les mises à jour vers un service
  - Vérification si la sortie de l'outil de vérification signature contient "Apple Root CA"
  - Possibilité d'installer d'anciennes versions, vulnérables

https://speakerdeck.com/patrickwardle/youre-muted-rooted

- Il reste des contournements, comme une "race condition"

Zimbra, exécution de commande à distance sans authentification (CVE-2022-27925)

- Découverte car massivement exploitée dans la nature
- Le PoC :
  - Contournement de l'authent avec les paramètres `account-name=valid_email` et `account-status=1`
  - Téléversement d'un ZIP exploitant un « directory traversal », ajoutant un « JSP »

https://github.com/vnhacker1337/CVE-2022-27925-PoC

Failles / Bulletins / Advisories
Réseau (principales failles)

VMWare, nombreuses vulnérabilités (CVE-2021-20031)

- Dont contournement de l'authent sur VMware Workspace ONE Access (CVE-2022-31656)
  - Le gestionnaire des identités 😱

https://www.cert.ssi.gouv.fr/avis/CERTFR-2022-AVI-703/
https://www.vmware.com/security/advisories/VMSA-2022-0021.html

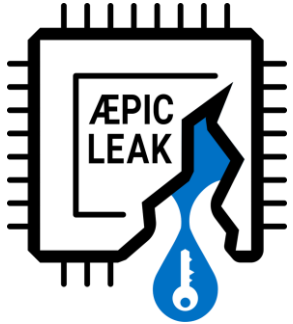
Failles / Bulletins / Advisories
*Spécial **CPU***

SQUIP / Side Channel Vulnerability (CVE-2021-46778)

- Accès à la mémoire, lors de la mesure de la file d'attente du planificateur d'exécution
  - Si le Simultaneous MultiThreading est activé (équivalent de l'hyper threading)
- Impacte : CPU **AMD** Zen 1, 2 et 3
- Correctif : pas de correctif, juste une recommandation pour les dev

https://www.phoronix.com/news/AMD-Side-Channel-SQUIP

AEPIC Leak / Architecturally Leaking Uninitialized Data from the Microarchitecture (CVE-2022-21233)



- Accès à la mémoire transitant entre L2 et L1
  - Du fait d'une mauvaise initialisation d'une zone mémoire des interruptions
  - Casse SGX (secure enclave)
  - PoC en 2 lignes de C : `u8* apic_base = map_phys_addr(0xFEE00000); dump(apic_base);`
- Impacte : CPU Intel de 10eme, 11eme et 12eme génération
- Correctif : microcode 20220809 (https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files/releases/tag/microcode-20220809)

https://aepicleak.com/
https://twitter.com/borrello_pietro/status/1557065849629863936

Failles / Bulletins / Advisories
*Spécial **CPU***

RetBleed (CVE-2022-29900 et CVE-2022-29901)

- 2 variantes de Spectre donnant accès à la mémoire
  - Du fait de l'exécution spéculative
- Impacte : CPU **Intel** et **AMD**
- Correctif : disponible mais avec une baisse de performance de 12% à 28%

https://comsec.ethz.ch/research/microarch/retbleed/

Phantom JMPS (CVE-2022-23825)

- 2 variantes de Spectre donnant accès à la mémoire
  - Du fait de l'exécution spéculative avec
- Impacte : CPU **Intel** et **AMD**
- Correctif : disponible mais avec une baisse de performance de 12% à 28%

https://comsec.ethz.ch/research/microarch/retbleed/

Failles / Bulletins / Advisories
*Spécial **CPU***

PACMAN pour macOS

- Contournement de PAC par un Oracle testant toutes les solutions (un peu bourrin 😁)
  - Nécessite une première vulnérabilité de lecture/écriture arbitraire
- Impacte : CPU **Apple M1**
- Correctif : pas de correctif

https://pacmanattack.com/

Failles / Bulletins / Advisories
Smartphones (principales failles)

Apple iOS 15.6.1 et macOS 12.5.1

- Vulnérabilités activement exploitées dans la nature
  - Depuis aout
- iOS 15.6.1 pour iPhone https://support.apple.com/en-us/HT213412
- iOS 15.6.1 pour iPad https://support.apple.com/en-us/HT213412
- macOS 12.5.1 pour mac https://support.apple.com/en-us/HT213413

iOS 15.6.1 and iPadOS 15.6.1

Released August 17, 2022

Kernel

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.

Description: An out-of-bounds write issue was addressed with improved bounds checking.

CVE-2022-32894: an anonymous researcher

WebKit

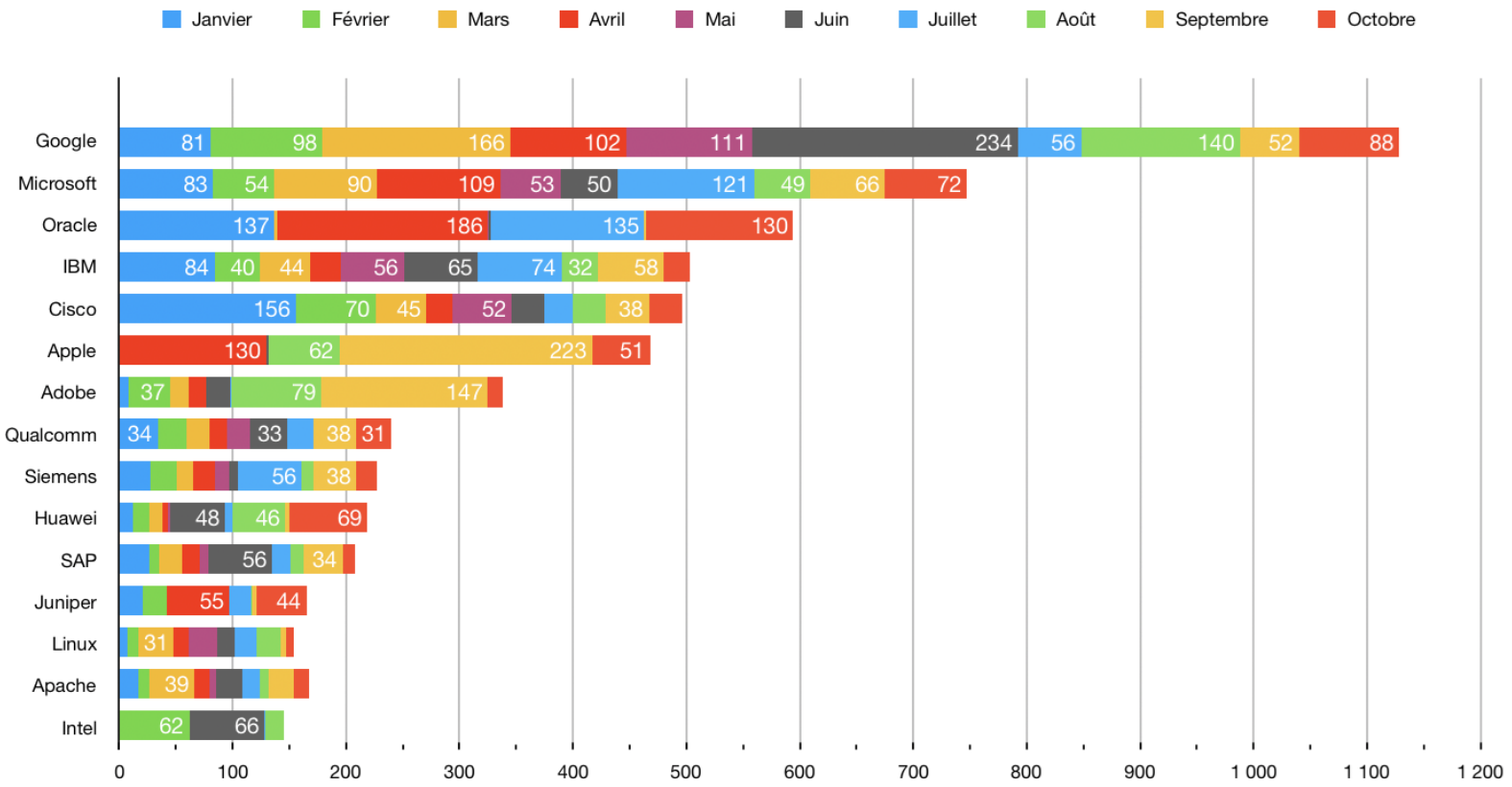
Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Description: An out-of-bounds write issue was addressed with improved bounds checking.

WebKit Bugzilla: 243557
CVE-2022-32893: an anonymous researcher

Stats du mois



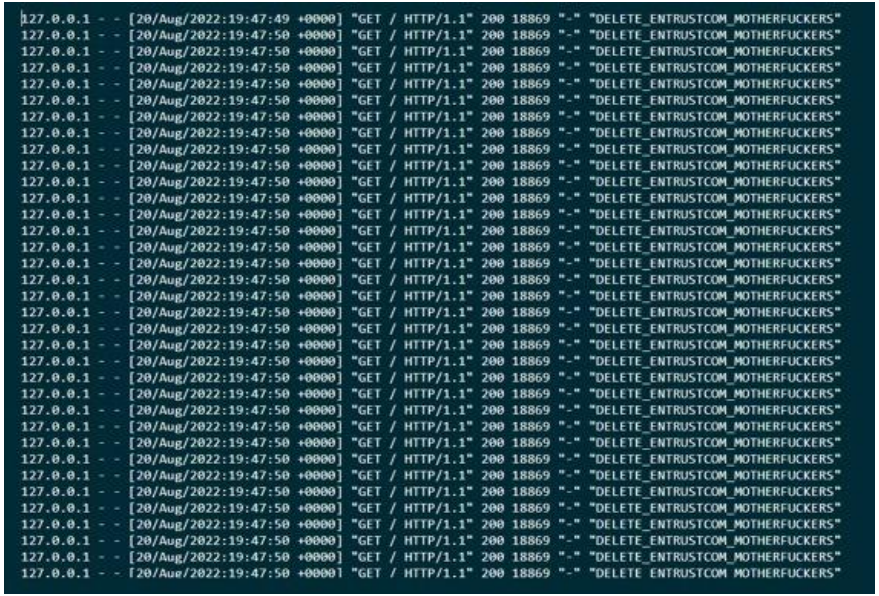
Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Entrust piraté par un affidé de LockBit

- Rançonnage classique
- DDoS des sites de LockBit
  - Par Entrust ?
- Publication d'un torrent de 343Go
  - Ressemble à des shares + 1 poste
  - Pas de com' d'Entrust

https://www.lemagit.fr/actualites/252523042/Quel-incident-de-cybersecurite-affecte-Entrust-depuis-un-mois



Piratage (d'un développeur) **de LastPass**

- Accès et vol de code source
  - A priori les mots de passe maître n'ont pas été volé car non stockés

https://blog.lastpass.com/2022/08/notice-of-recent-security-incident/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage de Plex et vol des données de 15m d'utilisateurs

- Vol du mail, nom et condensat du mot de passe
- 50% de leurs clients

https://arstechnica.com/information-technology/2022/08/plex-imposes-password-reset-after-hackers-steal-data-for-15-million-users/

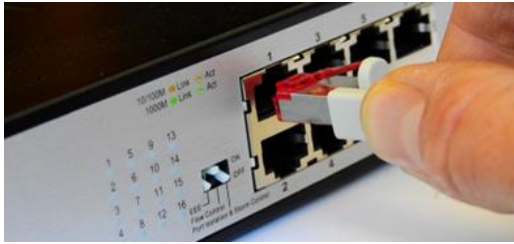
Falsification de preuves en Inde

- Contre des militants des droits de l'Homme, emprisonnés
  - Dépôts de faux documents de coup d'état sur leurs ordinateurs
  - Par le groupe "ModifiedElephant"
  - Les cibles déjà attaquées avec Pegasus de NSO
- Lié à la police indienne
  - L'opérateur a utilisé son n° de tel perso pour les comptes mails liés aux attaques (phishing)…
  - Avec sa photo sur Whatsapp

https://i.blackhat.com/USA-22/Thursday/US-22-Hegel-Charged-By-An-Elephant.pdf

https://www.01net.com/actualites/certains-policiers-sont-passes-maitres-en-fabrication-de-fausses-preuves-informatiques.html

Piratages, Malwares, spam, fraudes et DDoS
Piratages



France Connect désactivée

- Faille de sécurité suspectée
- Service de l'assurance maladie
  - De nombreux assurés ont été victimes de campagne de hameçonnage
  - Les escrocs prétextaient un faux renouvellement de la carte vitale ou un remboursement de soins.
  - Objectif : accéder à l'espace personnel des victimes pour modifier le RIB et ainsi percevoir les remboursements de soins médicaux dus.
  - La Cnam a coupé l'accès à son service via le portail France Connect
- Service des impôts
  - Attaques au site des impôts, (en utilisant le bouton de l'Assurance maladie)
  - But identique : réussir à changer le RIB pour encaisser l'argent reversé par l'administration fiscale.
  - Le fisc a choisi de désactiver le bouton de l'Assurance maladie pour se connecter au site des impôts
- Préjudice à plusieurs milliers d'euros.

https://demarchesadministratives.fr/actualites/assurance-maladie-pourquoi-la-connexion-via-france-connect-est-desactivee

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Raccoon Stealer v2, malware-as-a-Service

- Version précédentes actives depuis 2019
- Quelques évolutions :
  - Encodage Base64 + Chiffrement RC4
  - Chargement dynamique des fonctions WinAPI
  - Suppression de la dépendance du malware à l'API Telegram

https://www.zscaler.com/blogs/security-research/raccoon-stealer-v2-latest-generation-raccoon-family

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Quelqu'un dépose des centaines de noms de domaine…

- Proches de marques françaises :
  - cic-epargnrsalariale.fr
  - minecraft-frannce.fr
  - societegernerale.fr
  - wanatoo.fr

https://twitter.com/_mikolajek_/status/1550449744559984642 et https://ghostbin.me/62ddaff155404

- Un site pour les rassembler tous ;)

https://twitter.com/_mikolajek_/status/1561264538997198848

Attaque MFA CISCO

- vol de 2,75 Go de données comprenant plus de 3 000 fichiers
- notifications push d'authentification multifactorielle (MFA)
  - fatigue MFA et série d'attaques sophistiquées de phishing vocal

https://www.lemondeinformatique.fr/actualites/lire-cisco-compromis-par-le-gang-de-ransomware-yanluowang-87666.html

Piratages, Malwares, spam, fraudes et DDoS
Rançongiciel

Hôpital Corbeil-Essonnes

- 10m€ demandé, passée à 1m€ après négociation avec le GIGN
- Blocage réseau du SI
  https://www.usine-digitale.fr/article/l-hopital-de-corbeil-essonnes-en-mode-degrade-apres-une-attaque-par-rancongiciel.N2035587

Département Indre et Loire

- Rançongiciel Vice Society
- Corruption des 3/4 du SI (250 systèmes touchés)
- Versement allocations de 13 000 personnes
  https://www.francebleu.fr/infos/faits-divers-justice/indre-et-loire-encore-des-semaines-de-blocage-apres-la-cyberattaque-mais-les-allocations-seront-1657643957

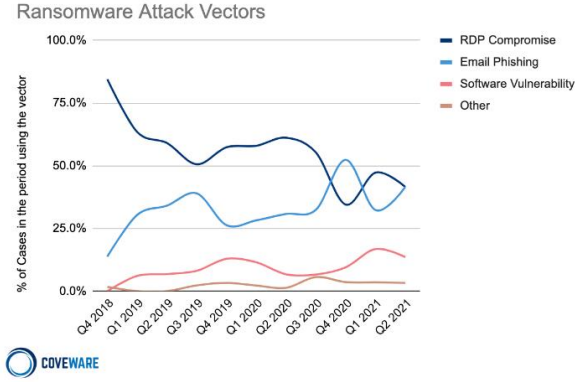
Damart se fait attacker par Hive, mais à un (bon) SOC

- Réponse à incident et coupure des accès sortants
  https://www.lemagit.fr/actualites/252524164/Cyberattaque-comment-Damart-a-coupe-lherbe-sous-le-pied-a-Hive

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Les principaux vecteurs d'attaque des cybercriminels

- 60% des compro. ont pour origine un actif exposé sur Internet
  https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority
- Le phishing est un vecteur mais pas le seul
  https://twitter.com/FuraxFox/status/1566067402156163072



Faux avis de passage mais vraie vulnérabilité !

- Faux avis de passage de la poste
- Lien + QRCode exploitant un open redirect sur laposte.net

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Attaque contre Signal

- Compromission de leur fournisseur de SMS : Twilio
  - Par Phishing et accès à la console du support clients
  - Enrôlement d'un autre terminal que celui de l'utilisateur
- 1 900 utilisateurs impactés, seulement sur leurs nouveaux messages
- Pour s'en prémunir il faut verrouiller l'enrôlement avec un PIN

https://support.signal.org/hc/en-us/articles/360007059792-Signal-PIN#manage_registration_lock
https://support.signal.org/hc/en-us/articles/4850133017242

Les suites…

- 130 autres entités ciblées
  - 22 opérateurs de télécommunications
  - +10k utilisateurs/comptes compromis
  - Collecte des informations volées sur un chan Telegram
- Cibles américaines et utilisant Okta

https://www.group-ib.com/media/0ktapus-campaign

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Contournement du MFA O365 ?

- Facile avec :
  - Un phishing
  - Un faux site mimant O365 ou le portail d'authent
  - Une sorte de MITM pour rejouer le MFA sur O365
- Fonctionne contre les MFA : HOTP, TOTP, notification, OTP par mail
  - Mais pas contre "FIDO / U2F / WebAuthn"

https://www.nextinpact.com/article/69741/une-vaste-campagne-phishing-contre-clients-microsoft-365-contourne-authentification-multifacteurs

La patronne de la Banque centrale européenne (BCE)

- Usurpation de l'identité d'Angela Merkel
- Contact de Christine Lagarde pour lui faire créer un compte de messagerie (whatsapp?)
- *"Nous n'avons rien de plus à dire car une enquête est en cours. »*

https://www.reuters.com/technology/ecbs-lagarde-is-targeted-cyber-attack-2022-07-12/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Les chaînes d'attaque par phishing… ça devient n'importe quoi

- .html > .zip > .lnk > .dll
  https://twitter.com/pr0xylife/status/1542905125873897473
- url > .zip > .iso > .lnk > .bat > .dll
  https://twitter.com/pr0xylife/status/1565029504317358080
- .zip > .iso > .lnk > .bat > wscript > .dll
  https://bazaar.abuse.ch/sample/369d2fd7604592ad2045949574012961651ec5cf8113b5d170e7956963c44ab1/
  https://twitter.com/pr0xylife/status/1559234481965436929
- GoogleDrive > .zip protégé par mot de passe > .lnk > .ps1 > .exe
  https://twitter.com/phage_nz/status/1559328175288889344
- .zip > .js > .ps1 > .vbs > .bat > .vbs > .bat > .ps1 > malware
  https://twitter.com/0xtoxin/status/1557463549517119489

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Ordinateurs quantiques & résistance

- Chiffrement SIKE post-quantic cassé en une heure sur un PC mono-cœur
  - Supersingular Isogeny Key Encapsulation par 17 cryptographes
  - Et c'est la deuxième fois en six mois ! No comment !
- Mais c'est une phase normale de cette sélection par le NIST

https://www.01net.com/actualites/un-chiffrement-du-futur-a-finalement-ete-casse-en-une-heure-sur-un-pc-monocoeur.html

Amélioration des attaques sur les algo post quantique

https://eprint.iacr.org/2022/214

https://eprint.iacr.org/2022/975

Voitures Tesla

- Model 3 : prise de contrôle par le composant multimédia (par Synacktiv)

https://www.youtube.com/watch?v=ZUs98Z-pIpY

- Model Y : ouverture et démarrage à distance

https://www.theverge.com/2022/9/12/23348765/tesla-model-y-unlock-drive-car-thief-nfc-relay-attack

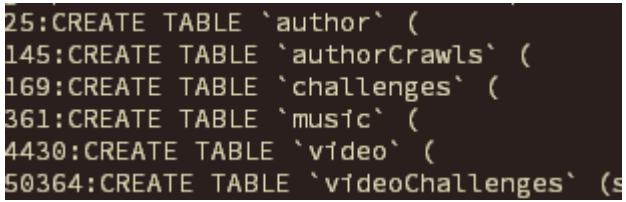
Piratages, Malwares, spam, fraudes et DDoS
Fuites de données

Fuite des clients OCD

- ~700 clients, avec les infos contacts

Fuite des utilisateurs de TikTok

- Sauvegarde SQL de 55Go



Fuite des utilisateurs de l'AD d'Altice

- Compromission totale du SI interne ?

La Poste Mobile (suite)

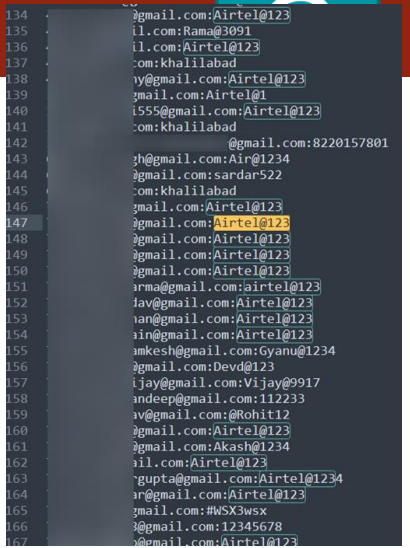
- Rançon initiale à $1,4m ? Négociations sans paiement pour le To

  https://www.lemagit.fr/actualites/252523794/La-Poste-Mobile-la-rancon-initiale-aurait-ete-de-14-million-de-dollars

Piratages, Malwares, spam, fraudes et DDoS
Fuites de données

AirTel ... pas besoin de vous demander votre mot de passe !

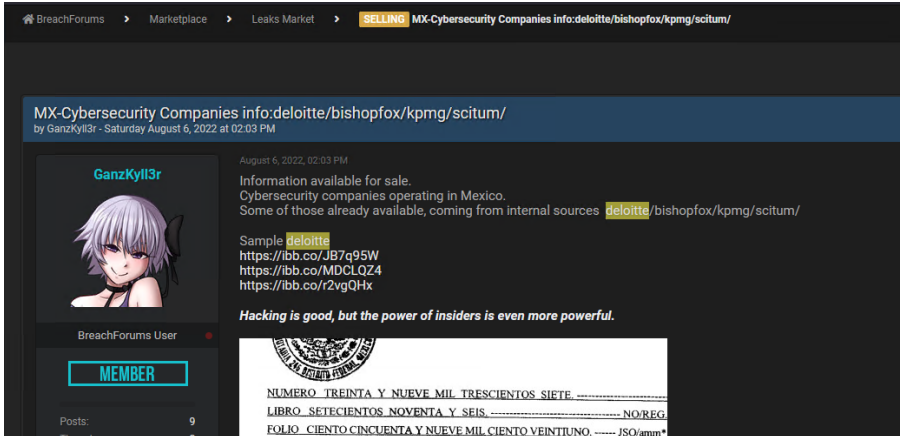
- Vol d'une base de donnée en 2021
- "dépersonnalisée" en août 2022
- ~18 000 clients (sur 48 000) ont le même mot de passe :
  - **Airtel@123**



Encore un leak Deloitte

- Deloitte/Bishopfox/KPMG/Scitum au Mexique

http://breached65xqh64s7xbkvqgg7bmj4nj7656hcb7x4g42x753r7zmejqd.onion/Thread-Selling-MX-Cybersecurity-Companies-info-deloitte-bishopfox-kpmg-scitum?highlight=deloitte



Piratages, Malwares, spam, fraudes et DDoS
Fuites de données

Twitter s'en fait voler

- Sequencement
  - Janvier 2022, vulnérabilité découverte (programme de Bug Bounty)
  - Juillet 2022, mise en vente d'informations compilées
  - Août 2022, Twitter révèle qu'une faille de sécurité : plus de 5,4 millions d'internautes concernés.
- Possible de déterminer l'identité de l'utilisateur derrière un compte

https://privacy.twitter.com/en/blog/2022/an-issue-affecting-some-anonymous-accounts

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Cloud, encore des pannes

- Teams https://twitter.com/MSFT365Status/status/1549934141738651648
- Google UK a cause de la chaleur https://www.clubic.com/pro/entreprises/google/actualite-430950-le-coup-de-chaud-d-un-data-center-google-cloud-a-londres-pour-quelles-consequences.html

  https://www.theregister.com/2022/07/19/google_oracle_cloud/
- Azure (à cause de DNS) https://twitter.com/GossiTheDog/status/1564576373628362753

Piratages, Malwares, spam, fraudes et DDoS
Publication

Guide pour sécuriser sa chaîne de développement

- Par la NSA suite aux attaques comme Solarwinds
- Granularité “étrange” (mix gouv/standard opérationnel)

https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

Être majeur selon la CNIL

- Elle demande en particulier à ce que les sites :
  - Ne collectent pas de pièce d’identité ;
  - N’estiment pas l’âge à partir de l’historique de navigation ;
  - Ne fassent pas de traitement de données biométrique.

https://www.nextinpact.com/article/48405/verification-dage-et-sites-pornos-cnil-trace-lignes-rouges

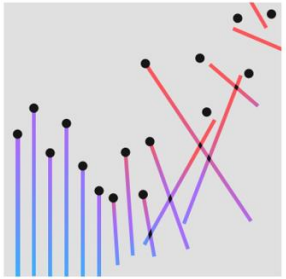
https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie

Piratages, Malwares, spam, fraudes et DDoS
Publication

Rapport sur le coût d'une violation de données IBM 2022

- A retenir
  - Infrastructures critiques à la traîne en matière de confiance zéro
  - **Il n'est pas payant de payer**
  - Immaturité de la sécurité dans le Cloud
  - L'IA et l'automatisation de la sécurité -> c’est l’avenir

https://www.ibm.com/downloads/cas/3R8N1DZJ



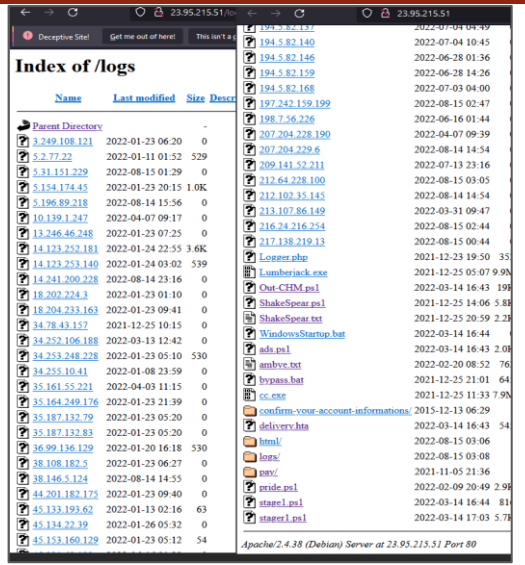
Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Blue Team "open directory" du site d'un attaquant #OpSecFail

- Scripts PowerShell, bypass UAC, logs des victimes…
- Près de 300 ip "à priori" compromises
  - Pensez à y rechercher les votres ici : https://pastebin.com/i7ZRsLrH

http://23.95.215.51/

https://twitter.com/whichbufferarda/status/1558885857611993089



AWK supporte unicode

- Ajouté par Brian Kernighan, à 80 ans

https://arstechnica.com/gadgets/2022/08/unix-legend-who-owes-us-nothing-keeps-fixing-foundational-awk-code/

Nouveautés
Divers

iOS16

- Mises à jour vraiment automatisées
- Bouton “panique” pour se déconnecter de tout voire réinitialiser tout
- Passkey, le FIDO d’Apple

  https://techcrunch.com/2022/09/12/ios-16-security-privacy/

RSSI/Risk Management
Techniques & outils

Stress Test … en Estonie

- Attaquants basés en Russie (Killnet)
  - DDoS sur 207 sites web
  - Paiement, banques, administrations et services publics
- Vous voulez un test (gratuit) de cyber-résilience ?
- Siim Sikkut* :
  - C’est facile, retirez une statue d'occupation soviétique
    - Deuxième fois que ça fonctionne pour l'Estonie !

https://www.euronews.com/next/2022/08/18/estonia-hit-by-most-extensive-cyberattack-since-2007-amid-tensions-with-russia-over-ukrain

** Siim Sikkut (ex-DSI du gouvernement de l'Estonie)*

Workers remove a Soviet T-34 tank installed as a monument in Narva, Estonia. Photograph: Sergei Stepanov/AP

Siim Sikkut
@sikkut

Business et Politique

Business
Monde

Le fond Thoma Bravo pourrait racheter Darktrace

- Darktrace côté en bourse à $4Mds (+20% suite à cette annonce)
  - Capitalisé à $18,2Mds
- Possède déjà PingIdentity, Sailpoint, Proofpoint, Sophos, McAfee, Venafi, Imperva, Veracode

https://www.lemondeinformatique.fr/actualites/lire-darktrace-bientot-dans-l-escarcelle-de-thoma-bravo-87688.html

Datadog rachète Seekret

- Société Israélienne spécialisée dans la supervision d'API grâce à eBPF

https://www.lemagit.fr/actualites/252524386/Avec-Seekret-Datadog-veut-suivre-a-la-trace-les-API-et-les-services

Droit / Juridique / Politique
Monde

Avisa, de nouveaux articles sur leurs “prestations”

- Après les faux articles (cf. revue du 12 juillet 2022)
- Manipulation des contenus de Wikipédia avec de “faux nez”

  https://reflets.info/articles/avisa-partners-la-desinformation-tendance-brune

- Wikipédia décide de bannir les comptes associés à Avisa
  - Rappel: FIC ∈ CEIS ∈ AVISA

  https://twitter.com/Wikipedia_fr/status/1558045273481437185

Recrutement de groupes de cybercriminels par Wagner

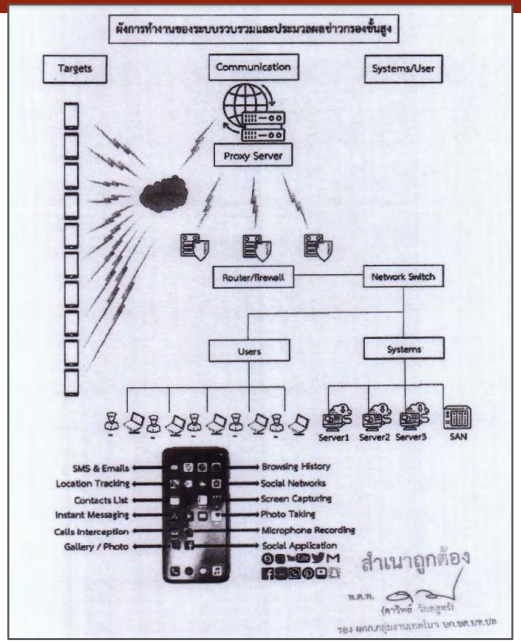
- Afin de mieux cadrer les cibles ?

  https://techinkers.com/russia-holds-back-its-cybercriminals-to-create-a-wagner-2-0-group/

Droit / Juridique / Politique
Monde

NSO Group et leur malware Pegasus

- Arrêt des négociations avec L3HArris pour leur rachat
  https://www.intelligenceonline.fr/surveillance--interception/2022/07/14/l3harris-nso--l-arret-des-negociations-agite-le-cyber-israelien,109799103-eve
- Pegasus trouvé aussi en thaïlande
  https://thehackernews.com/2022/07/pegasus-spyware-used-to-hack-devices-of.html
- Documentation de Pegasus, récupérée de la police Thaïlandaise
  https://twitter.com/maldr0id/status/1563610549853622272



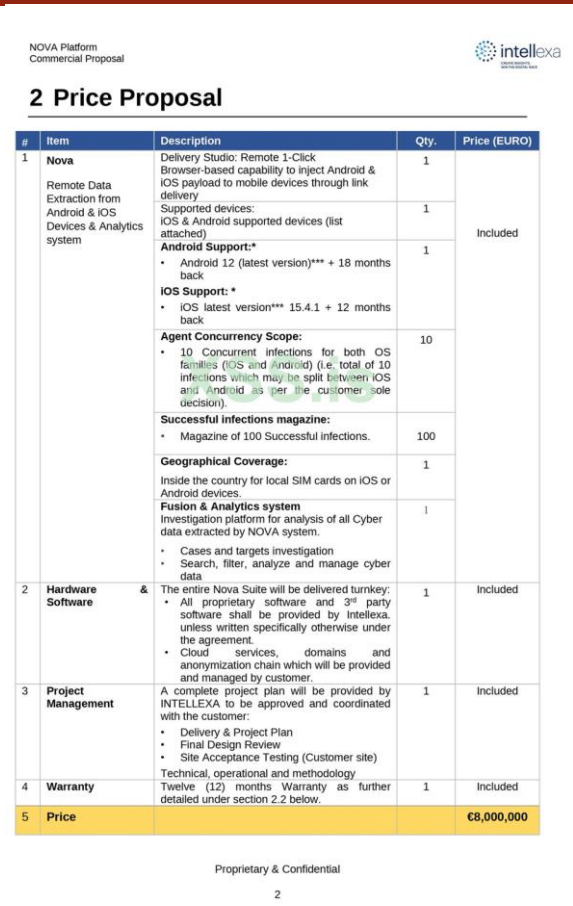
Droit / Juridique / Politique
Monde

Intellexa, publication de documents et proposition commerciale

- Publication des documents sur xss.is
  - Suite au piratage d'un client espagnol d'Intellexa
- Plateforme "Nova" : malware pour iOS et Android
  - Beaucoup de modèles supportés
- Pour 8m€ vous avez :
  - Compro de 10 cibles en même temps, avec des vulns 1-click
  - Support sur 12 mois

https://twitter.com/maddiestone/status/1562835519515480065
https://twitter.com/DrWhax/status/1562749756316585984

- Rappels :
  - Intellexa = fusion de Nexa et WiSpear (Israël) puis Senpai Technologies (anciens de l'Unité 8200)
  - Dirigeants poursuivis pour « `complicité d'actes de torture et de disparitions forcées` », cf. revue du 2021-09-14
  - Par les juges d'instruction du pôle « crimes contre l'humanité » du tribunal judiciaire de Paris
  - Suite à la vente de solution d'écoute par Nexa à l'Egypte



NOVA Platform
Commercial Proposal

intellexa

2 Price Proposal

#	Item	Description	Qty.	Price (EURO)
1	**Nova** Remote Data Extraction from Android & iOS Devices & Analytics system	Delivery Studio: Remote 1-Click Browser-based capability to inject Android & iOS payload to mobile devices through link delivery	1	Included
		Supported devices: iOS & Android supported devices (list attached)	1	
		Android Support:* • Android 12 (latest version)*** + 18 months back **iOS Support: *** • iOS latest version*** 15.4.1 + 12 months back	1	
		Agent Concurrency Scope: • 10 Concurrent infections for both OS families (iOS and Android) (i.e. total of 10 infections which may be split between iOS and Android as per the customer sole decision).	10	
		Successful infections magazine: • Magazine of 100 Successful infections.	100	
		Geographical Coverage: Inside the country for local SIM cards on iOS or Android devices.	1	
		Fusion & Analytics system Investigation platform for analysis of all Cyber data extracted by NOVA system. • Cases and targets investigation • Search, filter, analyze and manage cyber data	1	
2	**Hardware & Software**	The entire Nova Suite will be delivered turnkey: • All proprietary software and 3rd party software shall be provided by Intellexa. unless written specifically otherwise under the agreement. • Cloud services, domains and anonymization chain which will be provided and managed by customer.	1	Included
3	**Project Management**	A complete project plan will be provided by INTELLEXA to be approved and coordinated with the customer: • Delivery & Project Plan • Final Design Review • Site Acceptance Testing (Customer site) Technical, operational and methodology	1	Included
4	**Warranty**	Twelve (12) months Warranty as further detailed under section 2.2 below.	1	Included
5	**Price**			**€8,000,000**

Proprietary & Confidential

2

Droit / Juridique / Politique
Monde

Google, plainte à la CNIL

- De l’association NOYB ("None of your business")
- Pour spam des utilisateurs Gmail, contraire à l’ePrivacy
  - Diffusion de pub sans le consentement de l’utilisateur

https://www.usine-digitale.fr/article/noyb-porte-plainte-devant-la-cnil-contre-les-mails-publicitaires-de-google.N2036397

Fog Data Science

- Achats massifs de données de géolocalisation (venant d’app mobiles)
- Commercialisation d’un service de pistage vendu aux forces de l’ordre
  - Mais pas que…

https://twitter.com/furaxfox/status/1565485488382906368

Droit / Juridique / Politique
Monde

Cloud Act

- Il suffit d'avoir du matériel ou logiciel américain
  https://www.latribune.fr/technos-medias/internet/bleu-s3ns-pourquoi-les-offres-cloud-de-confiance-seront-certainement-soumises-au-cloud-act-928831.html

Accès aux données des clients des GAFAM ou entreprises US

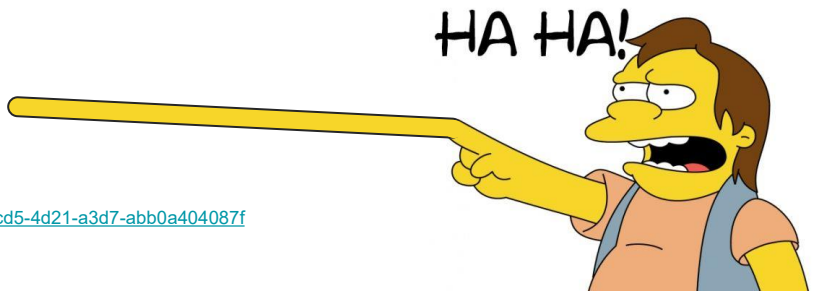
- Non, l'accès aux données des clients d'entreprises américaines (loi FISA) n'est pas un mythe
- Personne n'en parle mais personne ne refuse pour risquer de prendre 10 ans de prison
  https://twitter.com/herve_schauer/status/1567094135298920448

Droit / Juridique / Politique
Monde

Assurance Cyber = Ascenseur émotionnel

- 2017, NotPetya, des assureurs de Merck (victime) refusent de payer
  - Acte de guerre, le contrat ne s'appliquait pas
- 2022-01, AMRAE, l'assurance cyber pourrait disparaître
  https://www.cio-online.com/actualites/lire-oliver-wild-president-amrae--le-marche-de-la-cyber-assurance-n-existera-peut-etre-plus-l-an-prochain-13828.html
- 2022-02, Generali ne paiera pas les rançons
  https://www.lesechos.fr/finance-marches/banque-assurances/cyberattaques-lassureur-generali-tourne-le-dos-au-paiement-des-rancons-1383486
- 2022-06, Lloyd, pas de remboursement pour les victimes d'attaques étatiques

  - Qui va attribuer !!?
- 2022-09, Bercy veut autoriser l'indemnisation des rançons, à condition de déposer, pour :
  - Développer le business
  - Faciliter les investigations
  - Peu de risque que les **cybercriminels** en **profitent**
  - Pages 28 et 29, en 2.1.2, 2.1.3 et 2.1.4
    https://www.tresor.economie.gouv.fr/Articles/00367730-14c0-4303-95af-eeb6442fb19b/files/8a344142-fcd5-4d21-a3d7-abb0a404087f



Droit / Juridique / Politique
Monde

Assurance Cyber = Ascenseur émotionnel

Droit / Juridique / Politique
Monde

Accor, amende de 600k€ par la CNIL

- Inscription par défaut des clients à la newsletter
- Désinscription défectueuse

https://www.usine-digitale.fr/article/accor-ecope-d-une-amende-de-600000-euros-pour-violation-du-rgpd.N2034862

AG2R La Mondiale, amende de 1,75m€ par la CNIL

- Durée excessive de conservation des données personnelles
- Manque d'information lors du démarchage téléphonique par des sous-traitants

https://www.lemondeinformatique.fr/actualites/lire-rgpd-la-cnil-inflige-une-amende-de-1-75-meteuro-a-ag2r-la-mondiale-83675.html

Droit / Juridique / Politique
Monde

Criteo, amende potentielle de 60m€ de la CNIL

- Plainte de l'association Privacy International datant de 2018
- Traitements sans consentement ni information :
  - Tracking des personnes multi-appareils
  - Création de profils très précis et intrusifs
  - Partage (vente) des informations
- Plaintes également contre :
  - Quantcast (USA), Acxiom (Broker), Experian (credit rating) et Equifax (credit rating)

https://twitter.com/privacyint/status/1555572602273406976

https://www.usine-digitale.fr/article/la-cnil-pourrait-infliger-une-amende-de-60-millions-d-euros-a-criteo.N2032767

Vault7, jugement de l'agent de la CIA à l'origine de la fuite

- Reconnu coupable
- Risque 80 années de prison
- En cours de jugement aussi pour possession d'images et vidéos pédophiles

https://www.nextinpact.com/lebrief/69643/vault-7-presume-lanceur-dalerte-cia-reconnu-coupable

Droit / Juridique / Politique
Monde

Les incidents de sécurité dans le secteur de la santé ont doublé en un an

- 369 en 2020
- 733 en 2021
  - Incidents rencontrés par les prestataires de services informatiques
  - 52% d'origine malveillante
  - Nombreux vols d'identifiants

https://www.usine-digitale.fr/article/les-incidents-de-securite-dans-le-secteur-de-la-sante-ont-double-en-un-an.N1997407

Conférences

Conférences

Passée

- Troopers (très très offensif) : 27 juin au 1er juillet 2022
- Black Hat USA : 6 au 11 août 2022
- DefCon : 20, 11 au 14 août 2022
- Barbhack : 27 aout 2022

A venir

- FranSec : 13 et 14 septembre 2022
- DefCon Paris : ~~29~~ **19** septembre 2022
- Les Assises : 12 au 15 octobre 2022
- HexaCon : 14 et 15 octobre 2022

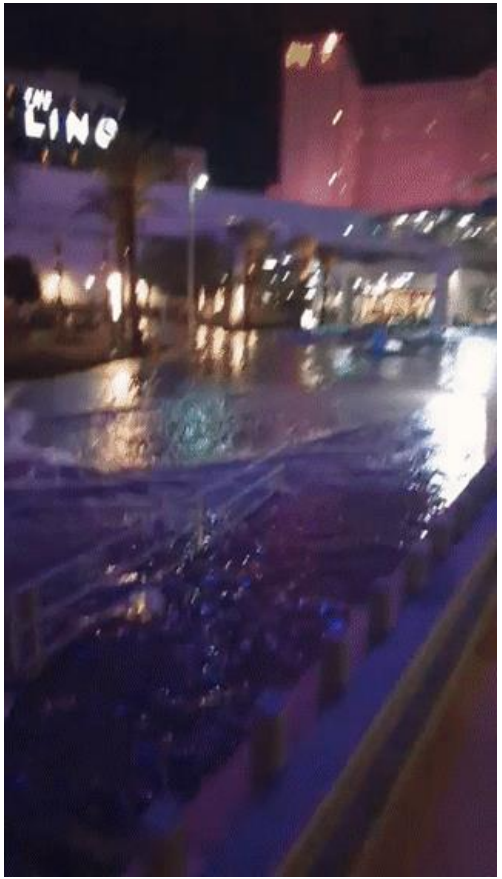
Conférences

Passée

- *Sthack : 20 mai 2022*
- *Troopers (très très offensif) : 27 juin au 1*
- *Black Hat USA : 6 au 11 août 2022*
- **DefCon : 20, 11 au 14 août 2022**

A venir

- *FranSec : 13 et 14 septembre 2022*
- *DefCon Paris : 29 septembre 2022*
- *Les Assises : 12 au 15 octobre 2022*
- *HexaCon : 14 et 15 octobre 2022*



Divers / Trolls velus

Divers / Trolls velus

Les trolls sont des cons 😂

- Étude de l’université d’Aarhus au Danemark
- Les « trolls » sur internet sont juste des gros cons aussi dans la vraie vie
  - Les gens ne seraient donc pas plus agressifs sur Internet que dans la vraie vie
  - Les gros cons sont juste plus visibles.

https://psyarxiv.com/hwb83/

Divers / Trolls velus

Utiliser un service tiers pour générer des QRCode…

- De vos secrets servant de base à l'authentification forte
- Qu'est ce qui pourrait mal se passer 🤦♂

https://twitter.com/adulau/status/1539516943388008449

Suivre les recommandations du NIST, c'est bien !

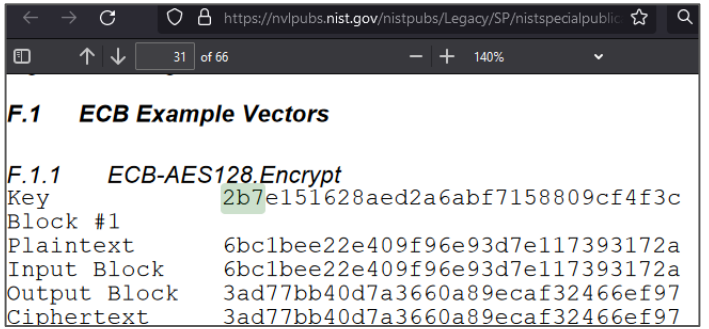
- Ne pas recopier bêtement la clef donnée en exemple c'est mieux 🤦♂
- Hyundai chiffre les firmwares de ses voitures avec la clef d'exemple du NIST

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

- Trouvé par greenluigi1 lors de l'analyse de wa Hyundai

https://hackaday.com/2022/07/18/hacker-liberates-hyundai-head-unit-writes-custom-apps/

https://programmingwithstyle.com/posts/howihackedmycar/



Divers / Trolls velus

Google TAG aux Pwnie Awards

- Et est nominé aux Pwnie Awards : Lamest Vendor Response
  - “unilaterally shutting down a counterterrorism operation”

https://twitter.com/PwnieAwards/status/1557268652197416966

- L’affaire à l’origine de cette nomination

https://www.technologyreview.com/2021/03/26/1021318/google-security-shut-down-counter-terrorist-us-ally/

Divers / Trolls velus

Latence du disque par vibrations … quand la musique est bonne

- # CVE-2022-38392
- *« Certains disques durs à 5400 tours/minute, destinés aux ordinateurs portables et autres PC à partir de 2005 environ, permettent à des attaquants physiquement proches de provoquer un déni de service (dysfonctionnement du dispositif et panne du système) via une attaque par fréquence de résonance avec le signal audio du clip vidéo Rhythm Nation »*.
- Ne faites pas trop de bruit dans les salles serveurs

https://twitter.com/MathisHammel/status/1560324797736812544

Divers / Trolls velus

Laisser ses secrets dans une application mobile

- 1859 app mobile trouvées avec des jetons AWS
  - 53% avec le même jeton (donc la même lib partagé, ce qui relativise ces résultats)

https://web.archivae.org/web/20211022075927/https://twitter.com/TheHackersNews/status/1451458130731102214

Patreon a viré toute son équipe sécu

- C’est surement qu’ils n’ont plus de vulnérabilités 🎉

https://twitter.com/wbm312/status/1567974063578185728

macOS, il y’aurait donc des virus !!?

- Apple inclut XProtect Remediator, un antivirus

https://www.01net.com/actualites/ni-vu-ni-connu-apple-deploie-un-veritable-antivirus-dans-ses-mac.html

Divers / Trolls velus

Facebook ne sait pas où sont vos données… ah ah ah… les gros nuls…

- Phrase exacte : `<<surpris s'il y avait ne serait-ce qu'une seule personne qui puisse répondre précisément à cette question>>`
- Normal sur une infra de cette taille et aussi complexe
  - Une seule personne seule ne peut pas tout connaître

https://www.vice.com/en/article/qjk3wb/facebook-engineers-admit-they-dont-know-what-they-do-with-your-data

Facebook se débarrasse de son équipe “Responsible Innovation”

- Mais rassurez vous, l’éthique perdurera 😂😂😂😂

https://www.nextinpact.com/lebrief/69932/facebook-met-fin-a-son-equipe-responsible-innovation-mais-promet-que-lethique-perdurera

Facebook supprime les ID statiques des utilisateurs

- Vous pouvez rangez vos leaks et outils d’OSINT

https://about.fb.com/news/2022/09/deterring-scraping-by-protecting-facebook-identifiers/

Divers / Trolls velus

Ouvrir un lien web dans les navigateur in-app

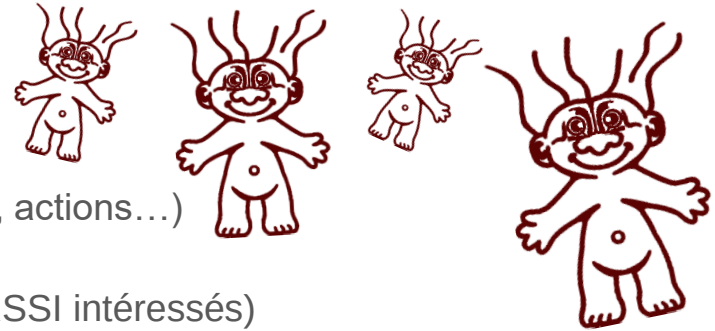
- Facebook, Instagram, TikTok…
  - Injection de Javascript, modification du contenu…
  - Enregistrement de vos saisies (mot de passe compris?)
  - Tracking, Tracking, Tracking…

https://krausefx.com/blog/announcing-inappbrowsercom-see-what-javascript-commands-get-executed-in-an-in-app-browser

https://www.01net.com/actualites/pourquoi-vous-devriez-eviter-douvrir-des-pages-web-dans-facebook-et-instagram.html

Divers / Trolls velus

RSSI = gros salaire + pression



- RSSI de grands comptes, dans le monde
- En 2022 :
  - USA ⇗+15%, moyenne $584k / an et $971k (avec primes, actions…)
  - UK ⇗+4%, $318k / an
  - Beaucoup de stress et de risques de burn out (selon les RSSI intéressés)
    - Comme le stress de dépasser 23kg de bagages de retour des Assises 😜 (©newsoft)
  - Beaucoup sont en poste depuis peu de temps

https://www.heidrick.com/en/insights/compensation-trends/2022-global-chief-information-security-officer-ciso-survey
https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2022-global-chief-information-security-officer-ciso-survey.pdf
https://www.lemondeinformatique.fr/actualites/lire-rssi-de-grand-compte-un-poste-bien-remunere-mais-sous-pression-en-2022-87709.html

Divers / Trolls velus

La carte des capacités offensive des états par Qihoo 360

- Liste des groupes et attaques associées

  https://apt.360.net/aptlist

- Y’a pas la france 😭

  https://news.sohu.com/a/583469076_362042

Divers / Trolls velus

Le FIRST publie TLP 2.0

- TLP:WHITE devient TLP:CLEAR
  - Car white s'oppose à black et donc c'est raciste 🙅‍♂️
- Il y'a donc 5 niveaux :
  - **TLP:RED** : uniquement pour une liste restreinte de gens nommés/listés
    - Comme à une conférence, devant 500 personnes 😁 #BoufConf
  - **TLP:AMBER** : les destinataires peuvent diffuser (limité à leur org/clients) si besoin d'en connaître
  - **TLP:AMBER+STRICT** : partage uniquement à l'organisation
    - Tellement mal nommé
  - **TLP:GREEN** : partage limité à sa communauté
  - TLP:CLEAR : Pour tout le monde
    - Par contre, la couleur reste le blanc 🙅‍♂️
- Et le FIRST fourni même les codes couleurs 🥲

https://www.first.org/tlp/

Questions ?

Des questions ?

- C’est le moment !

Des infos essentielles oubliées ?

- Contactez-nous

Prochaine Réunion

- Mardi 11 octobre 2022