Revue d'actualité de l'OSSIR

9 novembre 2021

Aurélien Denis

*Vladimir Kolla @mynameisv_*

Merci à la core team NoLimitSécu pour les derniers liens de ce midi 😁

Failles / Bulletins / Advisories

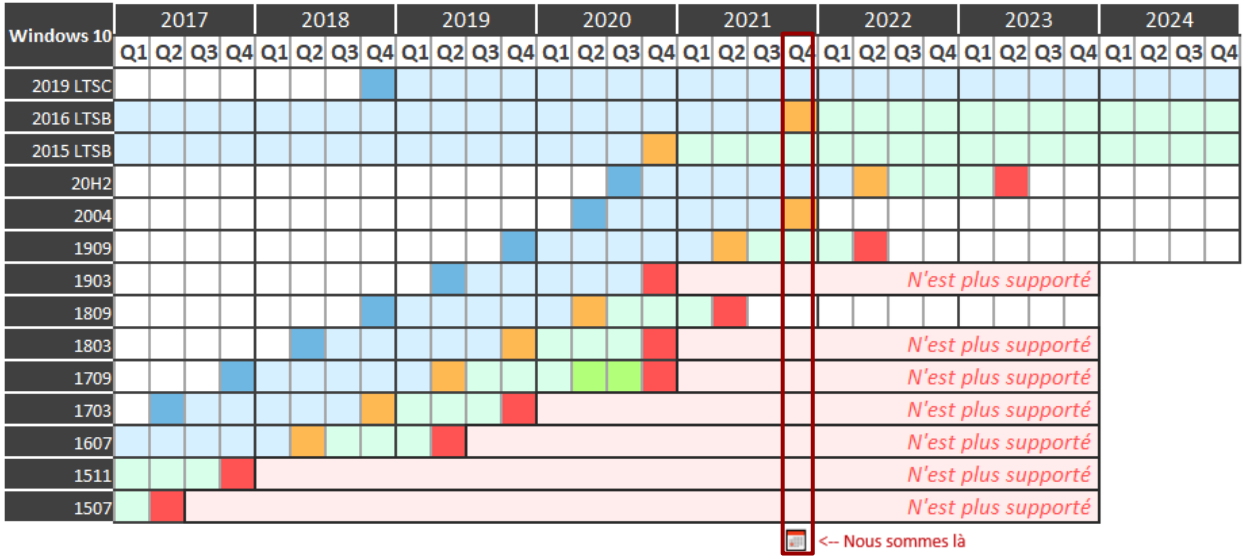
Failles / Bulletins / Advisories
Microsoft - Avis

En octobre :

- 71 vulnérabilités corrigées
- A retenir :
  - Spooler d'impression, nouveaux correctifs (CVE-2021-36970, CVE-2021-41332)
    - Les correctifs de sept. pour PrintNightmare cassent les impressions réseaux
      https://www.bleepingcomputer.com/news/microsoft/new-windows-10-kb5006670-update-breaks-network-printing/
  - Windows AppContainer, contournement du filtrage réseau (CVE-2021-41338)
    https://bugs.chromium.org/p/project-zero/issues/detail?id=2207
  - Exchange
    - exécution de code à distance (CVE-2021-26427) remonté par la **NSA** et déni de service (CVE-2021-34453)
    - élévation locale de privilèges (CVE-2021-41348)
  - Windows
    - élévation locale de privilèges (CVE-2021-41335
    - élévation locale de privilèges Win32k utilisée par le malware **MysterySnail** (CVE-2021-40449)
  - Windows Server, exécution de code à distance sur le DNS Windows (CVE-2021-40469)
  - SharePoint, execution de code à distance (CVE-2021-40487)
  - Microsoft Word, exécution de code à l'ouverture d'un document ou à la prévisualisation (CVE-2021-40486)
  - Windows Hyper-V
    - exécution de code à distance avec le service de virtualisation réseau (CVE-2021-40461)
    - exécution de code à distance (CVE-2021-38672)

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

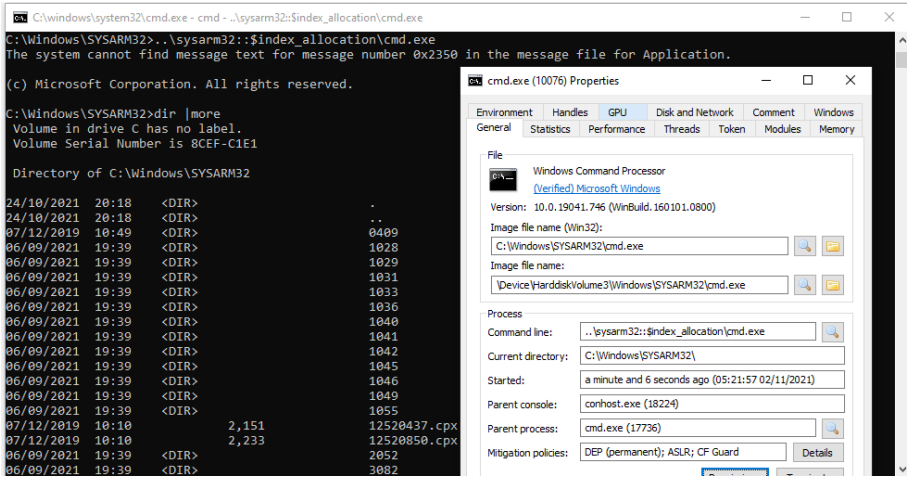
Failles / Bulletins / Advisories
Microsoft - Divers

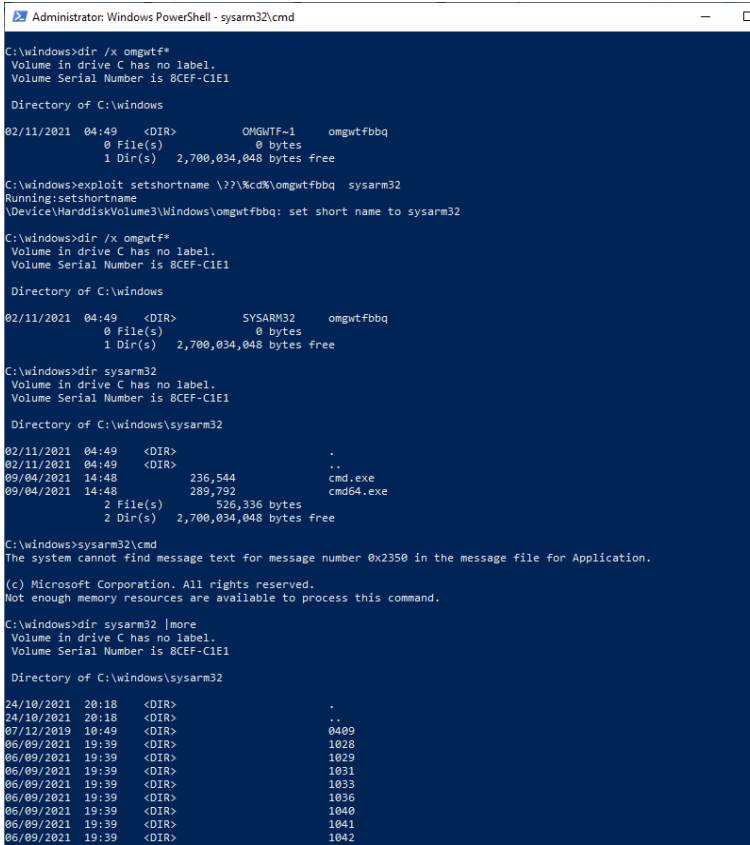
Faites-vous la différence entre un dossier 32-bits et 64-bits *(à part la taille)* ? Windows non plus

- Chaque dossier peut avoir deux noms
- *C:\Windows\system32 == C:\Windows\sysarm32*
  - *Si on crée un dossier dans C:\Windows (ici* `omgwtfbbq`*)*
  - Et qu'on met le shortname en "`sysarm32`" ---------->

https://twitter.com/jonasLyk/status/1455386495871750147

- Invisible pour le système





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

Gitlab CE, exécution de commande à distance (CVE-2021-22205)

- Téléversement d'une image contenant des métadonnées
  - Traité par ExifTool comme un fichier DjVu (sorte d'équivalent au PDF)
  - Contient une execution de commande (CVE-2021-22204 sur ExivTool)
- Découvert grâce à une revue des comptes d'administrateurs (j'ai enjolivé l'histoire 😁)
  - Exploité dans la nature *(mais pas du tout discrètement, pensez au moins à changer l'user-agent)*
  - Exploit : https://github.com/CsEnox/Gitlab-Exiftool-RCE/blob/main/exploit.py

https://security.humanativaspa.it/gitlab-ce-cve-2021-22205-in-the-wild/

Failles / Bulletins / Advisories
Réseau (principales failles)

Sonicwall 7.0 (CVE-2021-20031)

- Usurpation triviale de l'entête "host"
  - Permet de modifier la page web retournée en cas de réécriture du contenu

https://www.exploit-db.com/exploits/50414

SonicWall SMA 10.2.1.0-17sv, réinitialisation de mot de passe sans authentification (CVE-2021-20034)

- Grâce à un effacement arbitraire de fichier
  - Permettant de réinitialiser le mot de passe de l'administrateur
- Prise de contrôle du SonicWall à distance

https://attackerkb.com/topics/23t9VCbGzt/cve-2021-20034/rapid7-analysis

https://www.exploit-db.com/exploits/50430

```
curl -v --insecure "https://TARGET-IP/cgi-bin/handleWAFRedirect?hdl=../flash/etc/EasyAccess/var/conf/persist.db"
```

Failles / Bulletins / Advisories
Réseau (principales failles)

Cisco Policy Suite, une clef SSH laissée “encore” par défaut (CVE-2021-40119)

- Pour le compte root, avec sa partie privée bien sûr 😉

  https://thehackernews.com/2021/11/hardcoded-ssh-key-in-cisco-policy-suite.html

  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cps-static-key-JmS92hNv

Caméras IP, encore pleins de vulnérabilités

- Injections de commande, contournement de l’authentification….
- Publiées sur Metasploit

  https://twitter.com/ddouhine/status/1413075164955295745?s=11

Failles / Bulletins / Advisories
Smartphones (principales failles)

Apple iOS 15.1

- Exécution de code lors du traitement :
  - D'une image par le composant ColorSync (CVE-2021-30917)
  - D'un PDF par le composant CoreGraphics (CVE-2021-30919)
  - D'une archive par le composant FileProvider (CVE-2021-30881)
  - D'une page web par le navigateur Safari et son moteur WebKit (CVE-2021-30889)
  - D'un appel par le composant Voice Control (CVE-2021-30902)
    - Similaire aux vulnérabilités utilisées par Pegasus de NSO Group
    - Les détails sur la vulnérabilité : https://blog.zecops.com/research/use-after-free-in-voice-control-cve-2021-30902/
- Elevation locale de privilèges :
  - Par des appels au GPU (CVE-2021-30900, CVE-2021-30914)
  - Noyau (CVE-2021-30886, CVE-2021-30909, CVE-2021-30916)
  - Lors du traitement d'une image par le composant Image Processing (CVE-2021-30894)

https://support.apple.com/en-us/HT212867

Failles / Bulletins / Advisories
Compétitions

Tianfucup 2021

- Le Pwn2Own Chinois

  https://www.tianfucup.com/

- Kunlun Lab (Cyber Kunlun) a remporté la compétition
  - Total de prime de $654,500 sur les $1.88 millions
- Attention à la loi Chinoise sur les CVE

  https://portswigger.net/daily-swig/research-roadblock-security-pros-weigh-in-on-chinas-new-vulnerability-disclosure-law
- Tous vos actifs sont-ils à jour ? 😉

Target	2021 TFC Prize(RCE)	2021 TFC EXTRA Prize(RCE + Sandbox Escape)
Chrome	$50.000	$150,000
Safari	$40,000	$75,000
Adobe PDF Reader	$30,000	$40,000
Docker- CE	/	$60,000
Ubuntu 20/CentOS 8	/	$40,000
Microsoft Exchange Server 2019	$60,000	$200,000
Windows 10	$20,000	$40,000
VMware Workstation	/	$80,000
VMware ESXi	/	$180,000
Ubuntu + qemu-kvm	$60,000	$150,000
Parallels Desktop	/	$30,000
iPhone 12 pro	$120,000	$180,000
Smartphone Xiaomi Mi 11 (Android)	?	?
Synology DS220j	/	$10,000
ASUS Router AX56U	/	$10,000
Domestic vehicle	?	?

Failles / Bulletins / Advisories
Compétitions

Pwn2Own Austin 2021

- Spécial imprimantes, routeurs, smartphones…

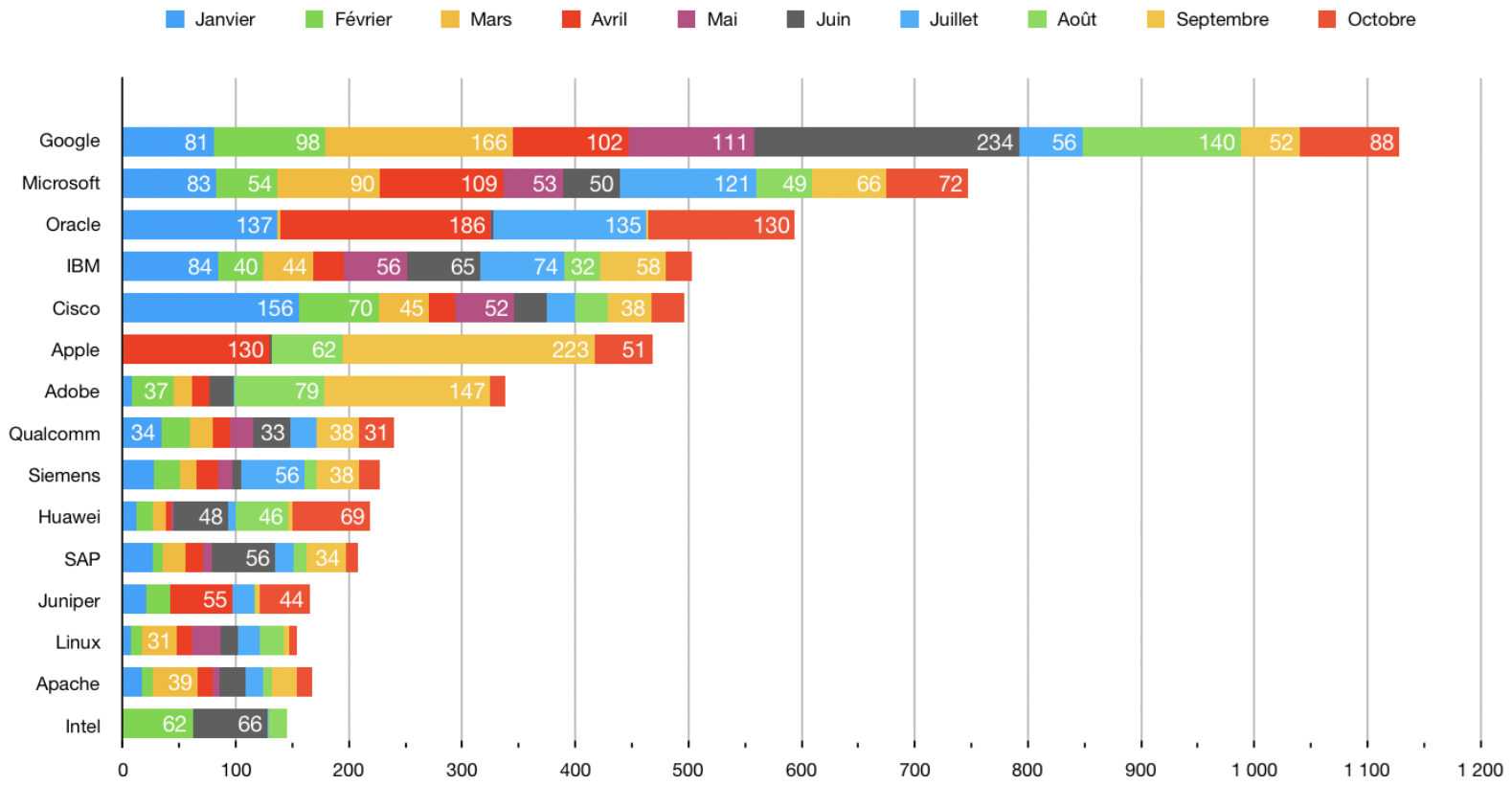
  https://www.zerodayinitiative.com/blog/2021/8/11/pwn2own-austin-2021-phones-printers-nas-and-more
- Quasiment tout a été piraté

  https://www.zerodayinitiative.com/blog/2021/11/1/pwn2ownaustin
- Très belle performance de Synacktiv

Contestant	Cash	Points
Synacktiv	$197,500	20
DEVCORE	$140,000	14
STARLabs	$112,500	12
Sam Thomas	$90,000	9
THEORI	$80,000	8
Bien Pham	$52,500	6.5
NCC Group	$60,000	6
trichimtrich	$40,000	5
Martin Rakhmanov	$40,000	4
Flashback	$33,750	3.75

Type	Modèle	Prix
Mobile Phones	Google Pixel 5	$50,000 (USD)
Mobile Phones	Samsung Galaxy S21	$150,000 (USD)
Mobile Phones	Apple iPhone 12	$150,000 (USD)
Home Automation	Portal from Facebook	$60,000 (USD)
Home Automation	Amazon Echo Show 10	$60,000 (USD)
Home Automation	Google Nest Hub (2nd Gen)	$60,000 (USD)
Home Automation	Sonos One Speaker	$60,000 (USD)
Home Automation	Apple HomePod mini	$60,000 (USD)
Printers	HP Color LaserJet Pro MFP M283fdw	$20,000 (USD)
Printers	Lexmark MC3224i	$20,000 (USD)
Printers	Canon ImageCLASS MF644Cdw	$20,000 (USD)
Televisions	Sony X80J Series - 43”	$20,000 (USD)
Televisions	Samsung Q60A Series – 43”	$20,000 (USD)
Routers	TP-Link AC1750 Smart Wi-Fi Router, from WAN	$20,000 (USD)
Routers	TP-Link AC1750 Smart Wi-Fi Router, from LAN	$5,000 (USD)
Routers	NETGEAR Nighthawk Smart Wi-Fi Router (R6700 AC1750), from WAN	$20,000 (USD)
Routers	NETGEAR Nighthawk Smart Wi-Fi Router (R6700 AC1750), from LAN	$5,000 (USD)
Routers	Cisco RV340, from WAN	$30,000 (USD)
Routers	Cisco RV340, from LAN	$15,000 (USD)
Routers	Mikrotik RB4011iGS+RM, from WAN	$30,000 (USD)
Routers	Mikrotik RB4011iGS+RM, from LAN	$15,000 (USD)
Routers	Ubiquiti Networks EdgeRouter 4, from WAN	$30,000 (USD)
Routers	Ubiquiti Networks EdgeRouter 4, from LAN	$15,000 (USD)
Network Attached Storage (NAS)	Synology DiskStation DS920+	$40,000 (USD)
[illegible]ached Storage (NAS)	My Cloud Pro Series PR4100 from WD	$40,000 (USD)
[illegible]ached Storage (NAS)	3TB My Cloud Home Personal Cloud from WD	$40,000 (USD)
[illegible]ached Storage (NAS)	3TB My Cloud Home Personal Cloud from WD	$45,000 (USD)
[illegible]age	1TB SanDisk Professional G-DRIVE ArmorLock SSD	$40,000 (USD)

Stats du mois



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Attaque de la banque nationale du pakistan

- Diffusion d’un malware par GPO
- Destruction du secteur de boot des ordinateurs, ATM...

https://therecord.media/destructive-cyberattack-hits-national-bank-of-pakistan/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

L’informatique ne marche plus très bien en Iran

- Problèmes de métro
  https://twitter.com/KhosroKalbasi/status/1456977068080701446
- Problèmes aux stations essence
  https://twitter.com/ReutersTech/status/1453128052783919110

Piratage de réseau 5G

- Alerte remontée par la NSA suite à des compromissions d’actifs exposés sur internet
  https://therecord.media/nsa-warns-of-threat-actors-compromise-entire-5g-networks-via-cloud-systems/
- La NSA et la CIA ont publié un guide de sécurisation des réseaux 5G
  - Identification des risques, des vulnérabilités, mesures de sécurité…

  https://www.cisa.gov/publication/5g-potential-threat-vectors

Piratage d’opérateurs télécom

https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Conti publie des données sur Mohammed Bin Salman

- Publication des données d'une entreprise anglaise de vente de diamants
  - Contenant des données sur MBS
  - Et s'en excuse 🤔
- Il est supposé que ce soit le Kremlin qui ait demandé à Conti de retirer ces données

https://www.vice.com/en/article/n7nw8m/conti-ransomware-hackers-apologize-to-arab-royal-families-for-leaking-their-data

Outil de déchiffrement pour Babuk

- Publié par Avast grâce à la fuite du code source

https://www.bleepingcomputer.com/news/security/babuk-ransomware-decryptor-released-to-recover-files-for-free/

Le trésor américain a identifié $5,2 milliards de transaction en bitcoin

- Liés à la cybercriminalité
- Entre janvier et juin 2021

https://therecord.media/treasury-said-it-tied-5-2-billion-in-btc-transactions-to-ransomware-payments/

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Shutdown de groupes majeurs

- Arrestation de 7 membres de Revil/GanCrab
  - 3 en Corée du Sud, 1 en europe, 1 au Koweit, 2 en Roumanie
- DarkMatter arrête ses opérations
- Le DoJ US déterminé à continuer ces takedowns

https://therecord.media/europol-seven-revil-gandcrab-ransomware-affiliates-were-arrested-in-2021/

https://therecord.media/blackmatter-ransomware-says-its-shutting-down-due-to-pressure-from-local-authorities/

https://www.sacbee.com/news/business/article255534846.html

Outil de déchiffrement pour DarkSide

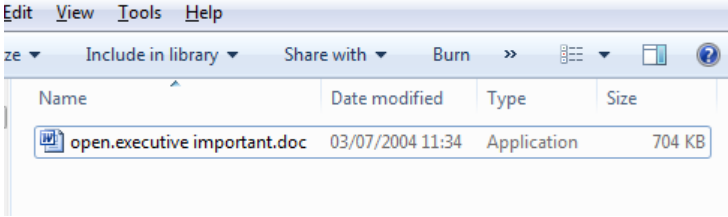
- Publié par BitDefender

https://www.bitdefender.com/blog/labs/darkside-ransomware-decryption-tool/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Le retour de Left-To-Right Override et ses amis (LRE, RLE, LRO, RLO)

- Caractères unicode d'inversion du sens de lecture
  - Utilisé par mail dans les années 2015-2016
- De retour pour cacher une porte dérobée dans du code
  - Principalement en manipulant des commentaires



https://twitter.com/aemkei/status/751905848725737472

```
public class TrojanSource {
    public static void main(String[] args) {
        String accessLevel = "user";
        if (accessLevel != "user") { // Check if admin
            System.out.println("You are an admin.");
        }
    }
}
```

```
public class TrojanSource {
    public static void main(String[] args) {
        String accessLevel = "user";
        if (accessLevel != "userRLO LRI// Check if adminPDI LRI") {
            System.out.println("You are an admin.");
        /* end admin only RLO { LRI*/
    }
}
```

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

npm ua-parser-js, encore une librairie “backdooréé”

- Le mainteneur annonce que son compte a été volé
  - Versions backdoorées : 0.7.29, 0.8.0 et 1.0.0
  - Téléchargement et exécution d’une DLL
- Librairie téléchargée 7 millions de fois / semaine

https://blog.xmco.fr/decouverte-de-logiciels-malveillants-embarques-dans-le-paquet-npm-ua-parser-js/

Arnaque au président par “deep voice”

- Usurpation de la voix du dirigeant
- Le coup classique de l'acquisition d’une entreprise nécessitant un transfert d’urgence

https://www.fredzone.org/une-banque-cambriolee-a-laide-du-deepfake-661/amp

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

Identités de tous les argentins sur le Darknet sombre des bas-fonds de DeepDarkWeb 4.0

- Mise en vente d'une base de données de TOUS les argentins
  - Sur le "Darknet"

https://www.lesnumeriques.com/vie-du-net/les-donnees-d-identite-de-tous-les-argentins-en-vente-sur-le-darknet-n170171.html

- Darknet… enfin juste sur Raidforum, publiquement accessible, sans authentification
  - darknet = raidforum + xss.is + eleaks.to + brute.pw 🤦‍♂️

https://twitter.com/timmedin/status/1454477809162854408?s=11

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Après Facebook, Korea Telecom rejoint le club des dénis de service par BGP

- Erreur de configuration BGP
- Impact sur 16,5 millions de clients pendant 40min

https://www.bleepingcomputer.com/news/technology/south-korean-telco-kt-suffers-nationwide-outage-after-routing-error/

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

Blue Team Un site qui mappe les LoLBAS

- Living off the Land ; Binaires légitimes utilisés de manière illégitimes
- Mappé sur la Matrice ATT&CK

https://lolbas-project.github.io/

Blue Team pour les nuls

- Vieux mais toujours intéressant à lire :

https://securitybytes.io/blue-team-fundamentals-4ee226368b7b

https://securitybytes.io/blue-team-fundamentals-part-two-windows-processes-759fe15965e2

MFT_Browser, pour naviguer dans une partition NTFS

- En évitant tout hooking, outil complexe...

https://github.com/kacos2000/MFT_Browser

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

Red Team contourner les EDR

- Classique :
  - En “hookant” plus bas
  - En appelant les API natives
- Mais une fois du code exécuté, c’est déjà quasiment perdu

https://medium.com/@omribaso/this-is-how-i-bypassed-almost-every-edr-6e9792cf6c44

Commando, la VM offensive de Mandiant

https://github.com/mandiant/commando-vm

L0phtCrack est à présent Open Source

https://l0phtcrack.gitlab.io/

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

LSASSY 3.0.0

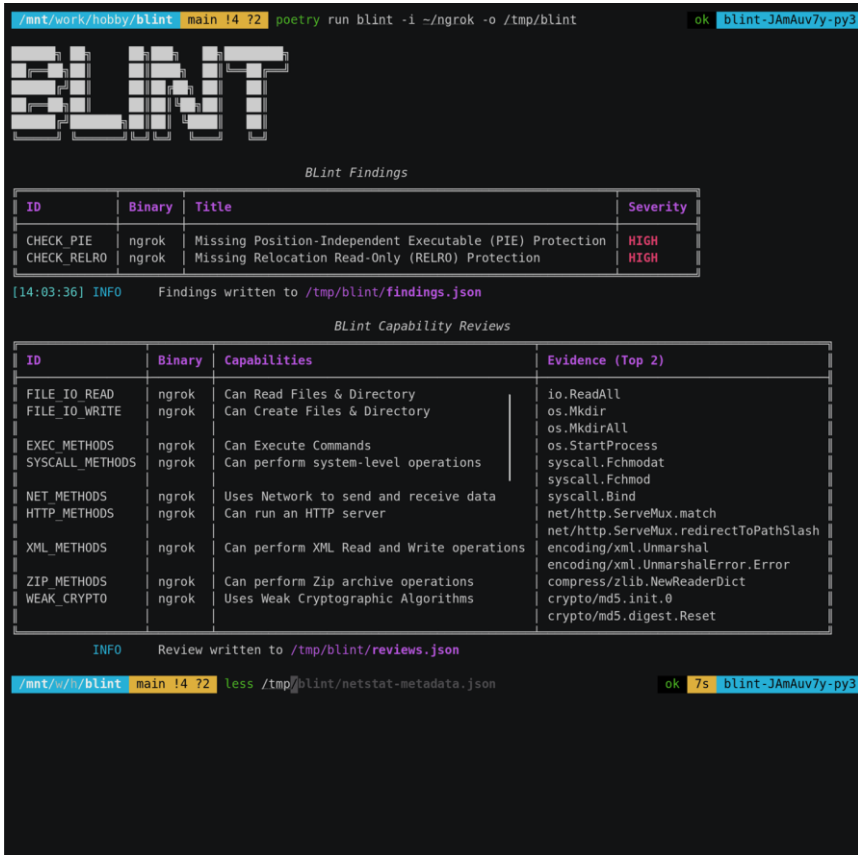
- Réécriture complète de l'outil
- Nouvelles méthodes de capture de la mémoire

https://github.com/Hackndo/lsassy/releases

BLINT : Récupérer des propriétés de binaires ELF

- Récupérer les informations d'un binaire

https://git.sr.ht/~prabhu/blint



Business et Politique

Business
Vie Privée

Alphabet : Perte de confiance dans Google à cause d'AMP

- Mais aussi:
  - Google aurait artificiellement augmenté le temps de réponse de ses régies publicitaires pour les sites qui n'utilisaient pas AMP
  - Computer Security Initiative Consultancy PTE. LTD. (Singapore)

https://wptavern.com/amp-has-irreparably-damaged-publishers-trust-in-google-led-initiatives

La CNIL australienne demande à Clearview AI de supprimer les données

- Concernant les australiens
- Impact vie privée **>** avantages d'intérêt public

https://www.nextinpact.com/lebrief/48713/la-cnil-australienne-ordonne-a-clearview-detruire-photos-ses-ressortissants

Business
Monde

Département du commerce US ajoute NSO Group dans sa “black list”

- Mais aussi:
  - Positive Technologies (Russie)
  - Computer Security Initiative Consultancy PTE. LTD. (Singapore)

https://www.federalregister.gov/documents/2021/11/04/2021-24123/addition-of-certain-entities-to-the-entity-list

NSO, rejet des demandes d’annulation des poursuites entamées par Whatsapp

- Plus de 1400 utilisateurs Whatsapp ciblés en 2019 (et detectés)
- NSO a demandé la même immunité que pour les agences étatiques et fonctionnaires
  - Rejet !

https://twitter.com/jsrailton/status/1457763675796803600?t=t4TCOaCTA-MrjVmlzz8wlQ&s=19

Business
Monde

ARM Chine fait secession

- La filiale dispose des licences
- Son PDG fait ses propres recherches et exploitations
  - Après avoir créé sa propre structure

https://www.numerama.com/tech/735628-le-casse-du-siecle-que-se-passe-t-il-avec-la-filiale-darm-en-chine.html

Scission entre Dell et VMWare

- VMWare acheté par EMC en 2004

https://www.nextinpact.com/lebrief/48539/la-scission-entre-dell-emc-et-vmware-sera-effective-1er-novembre

Business
Monde

ProofPoint vs VadeSecure, ce n’est pas fini

- ProofPoint demande $29m supplémentaires pour un nouveau préjudice
  - Venant s’ajouter aux $14m déjà validés

https://www.lalettrea.fr/entreprises_tech-et-telecoms/2021/10/29/proofpoint-demande-29-millions-de-dollars-supplementaires-a-vade-secure,109701880-art

ProofPoint et Gatewatcher signent un accord de partenariat

- Gatewatcher intégrera les règles de détection de ProofPoint

https://www.gatewatcher.com/newsroom/gatewatcher-et-proofpoint-sallient-pour-renforcer-la-detection-des-menaces-connues-et-inconnues-sur-le-trafic-reseau/

Droit / Politique
Monde

Quand le Cigref critique Microsoft Windows 11 sous l'angle de l'écologie

- Windows 11 nécessite de changer de matériel

  https://www.cigref.fr/empreinte-et-securite-numerique-les-associations-europeennes-dutilisateurs-interpellent-microsoft

Europol, arrestation de 12 cybercriminels

- Liés aux déploiement des ransomwares LockerGoga, MegaCortex et Dharma
- Il s'agirait des petites mains en charge des compromissions initiales

  https://www.presse-citron.net/ransomware-europol-annonce-larrestation-de-12-pirates-lors-dune-operation-coup-de-poing/

Opération "Dark HunTOR", arrestation de 150 cybercriminels par la gendarmerie

- Avec la coordination d'Europol
- Démantèlement des marchés DeepSea, Berlusconi, Dream, WallStreet, Dark Market et White House

  https://www.lefigaro.fr/actualite-france/spectaculaire-operation-au-coeur-du-darkweb-150-pirates-interpelles-20211026
- La vidéo d'une partie des arrestations

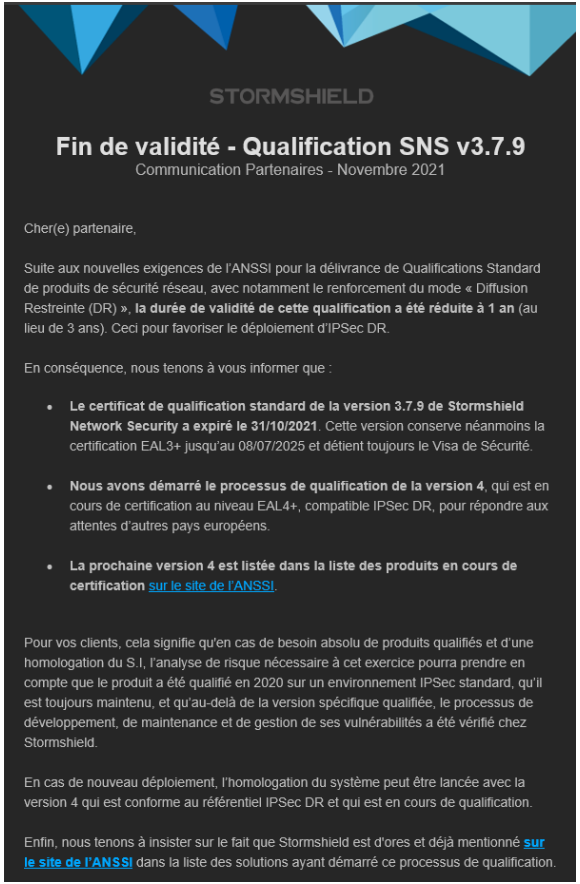
  https://www.youtube.com/watch?v=faPBYgHmaKM&t=38s

Droit / Politique
Monde

Les certifications de l’ANSSI passent de 3 à 1 an

- Stormshield n’est plus DR ni EAL4+

  https://www.ssi.gouv.fr/entreprise/produits-certifies/cc/les-evaluations/



STORMSHIELD

Fin de validité - Qualification SNS v3.7.9

Communication Partenaires - Novembre 2021

Cher(e) partenaire,

Suite aux nouvelles exigences de l'ANSSI pour la délivrance de Qualifications Standard de produits de sécurité réseau, avec notamment le renforcement du mode « Diffusion Restreinte (DR) », **la durée de validité de cette qualification a été réduite à 1 an** (au lieu de 3 ans). Ceci pour favoriser le déploiement d'IPSec DR.

En conséquence, nous tenons à vous informer que :

- **Le certificat de qualification standard de la version 3.7.9 de Stormshield Network Security a expiré le 31/10/2021**. Cette version conserve néanmoins la certification EAL3+ jusqu'au 08/07/2025 et détient toujours le Visa de Sécurité.
- **Nous avons démarré le processus de qualification de la version 4**, qui est en cours de certification au niveau EAL4+, compatible IPSec DR, pour répondre aux attentes d'autres pays européens.
- **La prochaine version 4 est listée dans la liste des produits en cours de certification** sur le site de l'ANSSI.

Pour vos clients, cela signifie qu'en cas de besoin absolu de produits qualifiés et d'une homologation du S.I, l'analyse de risque nécessaire à cet exercice pourra prendre en compte que le produit a été qualifié en 2020 sur un environnement IPSec standard, qu'il est toujours maintenu, et qu'au-delà de la version spécifique qualifiée, le processus de développement, de maintenance et de gestion de ses vulnérabilités a été vérifié chez Stormshield.

En cas de nouveau déploiement, l'homologation du système peut être lancée avec la version 4 qui est conforme au référentiel IPSec DR et qui est en cours de qualification.

Enfin, nous tenons à insister sur le fait que Stormshield est d'ores et déjà mentionné **sur le site de l'ANSSI** dans la liste des solutions ayant démarré ce processus de qualification.

Conférences

Conférences

Passée

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

A venir

- Le Hack
- SSTIC 2021 - en distanciel, du 2 au 4 juin 2021
- Sthack - 15 octobre 2021
- Insomni’hack - en 2022

Divers / Trolls velus

Divers / Trolls velus

Google supprime tout HackerNews (dont les sauvegardes)

- Service rétabli dans la journée

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

Gagnez $10 millions… en donnant des informations sur DarkSide

- Groupe ayant attaqué le “Colonial Pipe”

  https://www.state.gov/darkside-ransomware-as-a-service-raas/

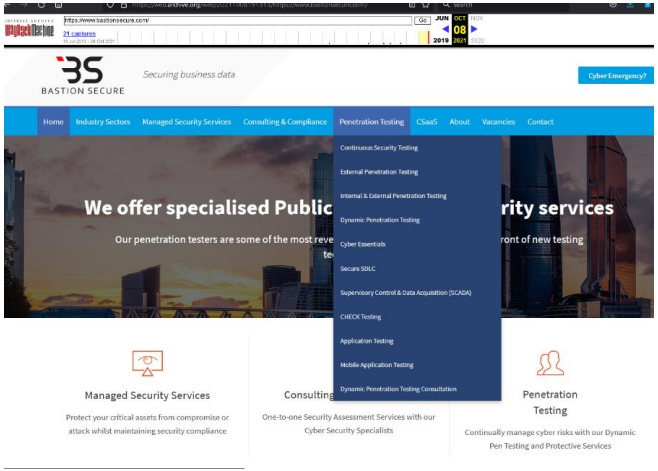
Divers / Trolls velus

Bastion Secure recrute

- Avec des offres en Russe
- Sauf qu'il s'agissait de FIN7
- Pour manipuler des chercheurs
  - Et leur faire mener des attaques de rançongiciel

https://twitter.com/campuscodi/status/1451241854142492684

https://web.archive.org/web/20211008191313/https://www.bastionsecure.com/



La Russie extrade un de ses cybercriminels vers les USA

- Vladimir Dunaev, 38 ans, membre de Trickbot

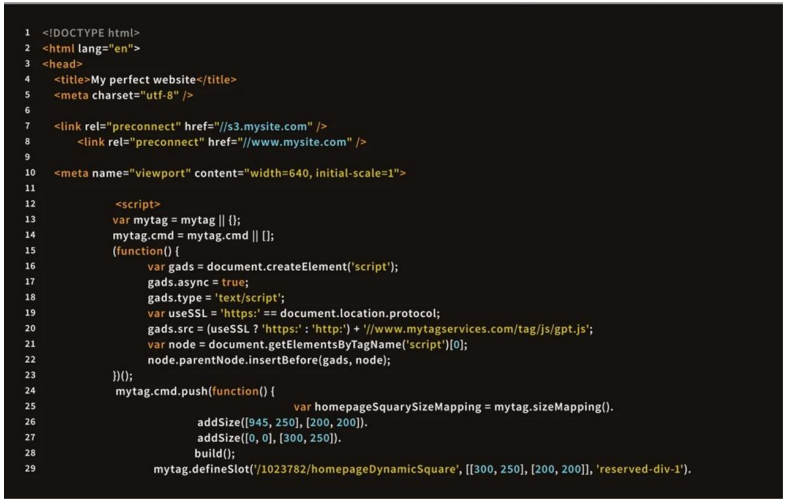
https://www.justice.gov/opa/pr/russian-national-extradited-united-states-face-charges-alleged-role-cybercriminal

Divers / Trolls velus

Cyberhack : Appuyer sur F12 fera de vous un criminel dans le Missouri

- Un journaliste américain est parvenu à récupérer des numéros de sécurité sociale
- Grâce à une technique hautement avancée 😳
  - Clic droit -> Afficher le code source ou F12
- Le gouverneur a annoncé vouloir porter plainte contre le journaliste

https://techcrunch.com/2021/10/15/f12-isnt-hacking-missouri-governor-threatens-to-prosecute-local-journalist-for-finding-exposed-state-data



```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>My perfect website</title>
  <meta charset="utf-8" />

  <link rel="preconnect" href="//s3.mysite.com" />
      <link rel="preconnect" href="//www.mysite.com" />

  <meta name="viewport" content="width=640, initial-scale=1">

            <script>
            var mytag = mytag || {};
            mytag.cmd = mytag.cmd || [];
            (function() {
                  var gads = document.createElement('script');
                  gads.async = true;
                  gads.type = 'text/script';
                  var useSSL = 'https:' == document.location.protocol;
                  gads.src = (useSSL ? 'https:' : 'http:') + '//www.mytagservices.com/tag/js/gpt.js';
                  var node = document.getElementsByTagName('script')[0];
                  node.parentNode.insertBefore(gads, node);
            })();
             mytag.cmd.push(function() {
                                    var homepageSquarySizeMapping = mytag.sizeMapping().
                        addSize([945, 250], [200, 200]).
                        addSize([0, 0], [300, 250]).
                        build();
                   mytag.defineSlot('/1023782/homepageDynamicSquare', [[300, 250], [200, 200]], 'reserved-div-1').
```

Divers / Trolls velus

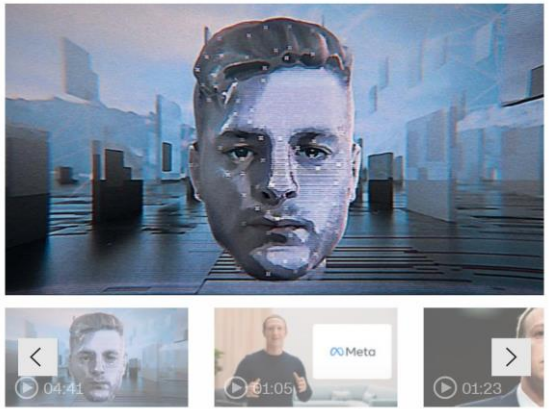
<<Promis nous arrêtons la reconnaissance faciale>>

- Facebook va arrêter, pas Meta

Facebook is shutting down its facial recognition software 😘😘😘😘😘😘😘😘

By Rachel Metz, CNN Business

Updated 2011 GMT (0411 HKT) November 2, 2021



Meta to continue use of facial recognition technology

Mikey Campbell | Nov 04, 2021

Meta

AppleInsider is supported by its audience and may earn commission as an Amazon Associate and affiliate partner on qualifying purchases. These affiliate partnerships do not influence our editorial content.

Facebook this week announced that it will no longer deploy facial recognition technologies on its platform, but the social network's parent company, Meta, said that the commitment

Divers / Trolls velus

~~GAFAM~~ **MAGMA**

- Meta
- Amazon
- Google
- Microsoft
- Apple

Divers / Trolls velus

Le bon vieux temps 😁

- Devinez à quoi ça fait référence: FCKGW-RHQQ2-YXRKT-8TG6W-2B7Q8
  - Indice : cela fait 20 ans (devils0wn)
- “Smashing the Stack for Fun and Profit” a 25 ans
  http://phrack.org/issues/49/14.html#article
  https://www.arsouyes.org/phrack-trad/phrack49/phrack49_0x0e_SlasH.txt

Prochaines réunions

Prochaine réunion

- 14 décembre 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 ?