Revue d'actualité de l'OSSIR

09 janvier 2024

Jérémy De Cock
Christophe Chasseboeuf
Vladimir Kolla
Marc-Antoine Ledieu

Meilleurs voeux !

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de septembre, 34 vulnérabilités patchées dont

- 1 zero-day :
  - [**CVE-2023-20588**] “division par zero” sur certains processeurs AMD : leak de données
    - Nécessite un accès local à la machine
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2023-35630,35641 & 36397**] Internet Connection Sharing (ICS) : RCE
    - Service désactivé par défaut
  - [**CVE-2023-36019**] Power Platform Connector : spoofing
  - [**CVE-2023-35628**] Windows MSHTML Platform Remote : RCE

https://www.lemondeinformatique.fr/actualites/lire-patch-tuesday-decembre-2023-4-failles-critiques-corrigees-92421.html

Failles / Bulletins / Advisories
Microsoft - Divers

Désactivation du protocole MSIX par Microsoft

- **CVE-2021-43890** dans Windows AppX
  - Permettant de déployer des malwares…
  - Tout en bypassant les sécurités de Microsoft (dont SmartScreen)
- Déjà désactivé en février 2022 car exploité par Emotet
  - Mais également Bazarloader & Trickbot
- Et désactivé de nouveau en décembre 2023 ?
  - Quand a-t-il été de nouveau activé ? Et pourquoi ? 😑
- Assurez-vous que App Installer soit en version **1.21.3421.0**

https://www.it-connect.fr/windows-microsof-desactive-msix-protection-malwares/

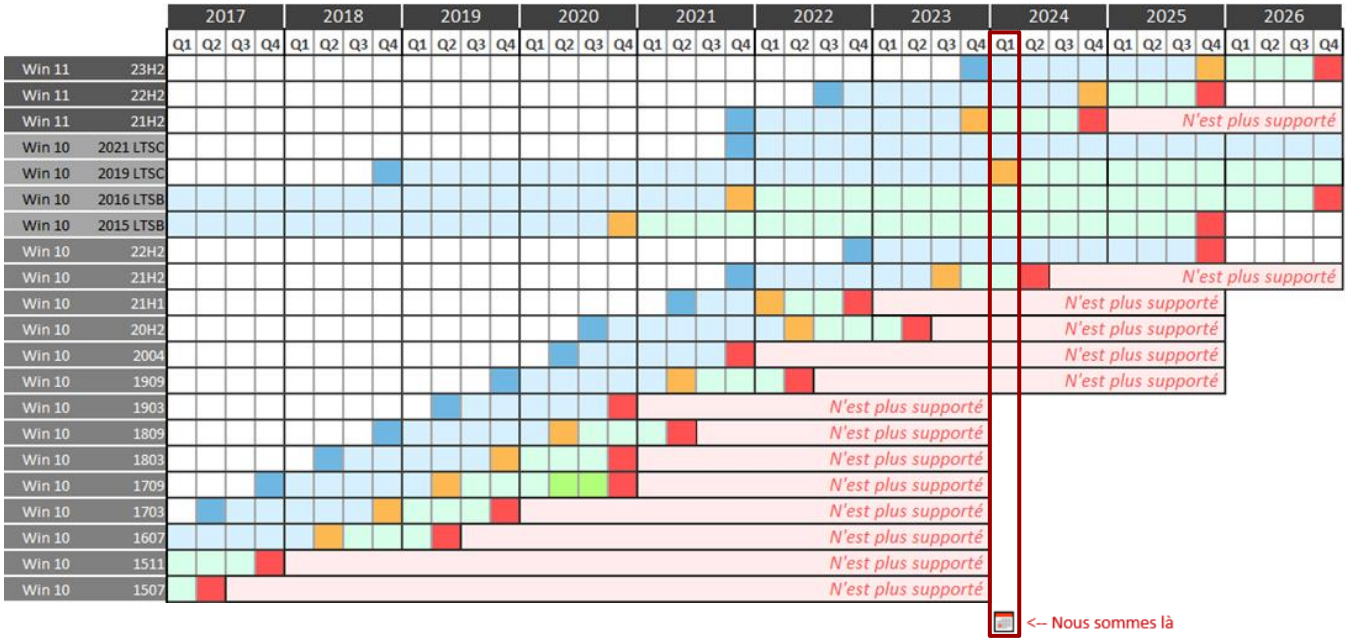
PoC pour les vulnérabilités SharePoint (CVE-2023-29357 et CVE-2023-24955)

- Execution de code à distance sans authentification

https://securityonline.info/poc-released-for-sharepoint-pre-auth-rce-chain-cve-2023-29357-cve-2023-24955/

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 / 11 en couleurs



Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
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 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 18 octobre 2022	mardi 14 octobre 2025	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	mardi 10 mai 2022
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	mardi 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
mercredi 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	mardi 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
Systèmes

Plusieurs vulnérabilité du côté de pfSense

- 3 vulnérabilités trouvées :
  - [**CVE-2023-42325**] XSS réfléchie, présente dans *status_logs_filter_dynamic.php*
  - [**CVE-2023-42327**] XSS réfléchie, présente dans *getserviceproviders.php*
  - [**CVE-2023-42326**] RCE **authenticated**, présente dans *_gif_edit.php* et *_gre_edit.php*
- Cibles ?
  - pfSense CE 2.7.0 et -
  - pfSense Plus 23.05.1 et -
- Mettez à jour
  - pfSense CE 2.7.1
  - pfSense Plus 23.09
- Vulns connues depuis le 03/07/2023 et maj publiée en 11/2023…
- 1500 firewalls exposés et vulnérables (source : Shodan)

https://www.it-connect.fr/environ-1-500-firewalls-pfsense-vulnerables-a-une-execution-de-code-a-distance/

Failles / Bulletins / Advisories
Systèmes

Apple, 30 novembre 2023

- Les mises à jour :
  - Safari 17.1.1 -> mettre à jour en Safari 17.1.2 https://support.apple.com/en-us/HT214033
  - iOS 17.1.1 -> mettre à jour en iOS 17.1.2 https://support.apple.com/en-us/HT214031
  - iPadOS 17.1.1 -> mettre à jour en iPadOS 17.1.2 https://support.apple.com/en-us/HT214031
  - macOS Sonoma 14.1.1 -> mettre à jour en macOS Sonoma 14.1.2 https://support.apple.com/en-us/HT214032
- Les vulnérabilités :
  - CVE-2023-42916, fuite d'information mémoire dans Safari
  - CVE-2023-42917, exécution de code à la consultation d'une page web

Failles / Bulletins / Advisories
Systèmes

Apple, 11 décembre 2023

- Les mises à jour :
  - iOS 17.1.2 -> mettre à jour en iOS 17.2 https://support.apple.com/en-us/HT214035
  - macOS Sonoma 14.1.2 -> mettre à jour en macOS Sonoma 14.2 https://support.apple.com/en-us/HT214036
  - …
- Les vulnérabilités :
  - **Bluetooth**, contournement de l'authentification d'un périphérique
    - Envoie de frappes de clavier pour générer des actions (CVE-2023-45866) https://github.com/skysafe/reblog/tree/main/cve-2023-45866 ;
  - **Safari** (WebKit), exécution de code à la consultation d'une page web (CVE-2023-4289)
  - **Noyau** iOS/macOS, évasion de la sandbox des applicat… (CVE-2023-42914)
    - La vulnérabilité a été trouvée par Eloi de Synacktiv 👍🐱 
  - **AppleGraphicsControl** et AppleVA, multiples exécutions de code
  - **Vim**, exécution de code à l'ouverture d'un fichier spécialement formaté (CVE-2023-5344)

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Nouvelle 0-day sur Chrome (CVE-2023-7024)

- Corrigée par Google 7h après en avoir eu connaissance 👏
- Heap-based buffer overflow dans le framework WebRTC
  - Framework également utilisé par Microsoft Edge, Mozilla Firefox, Safari…
  - Permet d'avoir une RCE sur le système de la victime
- Mettez à jour
  - Windows : 120.0.6099.129/130
  - Linux & macOS : 120.0.6099.129
- 8ème et dernière faille de sécurité 0-day de l'année !

https://www.bleepingcomputer.com/news/security/google-fixes-8th-chrome-zero-day-exploited-in-attacks-this-year/

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

Faille critique découverte dans Apache Struts (CVE-2023-50164)

- Permet d'avoir une RCE unauthenticated
  - 1ère étape : mise en place d'une backdoor via une "Path Traversal"
  - 2ème étape : exécution de code à distance
- Affecte plusieurs branches
  - 2.0.0 à 2.5.32
  - 6.0.0 à 6.3.0.1
  - 2.0.0 à 2.3.37 (versions qui ne sont plus supportées !)

https://github.com/jakabakos/CVE-2023-50164-Apache-Struts-RCE (POC)

https://www.it-connect.fr/les-cybercriminels-exploitent-activement-la-faille-critique-decouverte-dans-apache-struts/

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

Attaque Terrapin, le nouveau ennemi d'OpenSSH ?

- Liée à 3 failles de sécurité : CVE-2023-48795, CVE-2023-46445 & CVE-2023-46446
- Attaque de type "man-in-the-middle" (couche réseau)
  - Permettant d'intercepter et de modifier l'échange client / serveur lors du handshake
- Contrainte :
  - La connexion doit être sécurisée avec ChaCha20-Poly1305 ou CBC + "Encrypt-then-MAC"
- But ?
  - Altérer les données échangées + RCE
- 77% des serveurs avec le service SSH exposé seraient vulnérables
  - Version OpenSSH < 9.6
  - Risque réel mais dans les faits, quasi inexploitable !!!

https://github.com/RUB-NDS/Terrapin-Scanner (outil d'analyse sur Windows, Linux & macOS)

https://www.bleepingcomputer.com/news/security/terrapin-attacks-can-downgrade-security-of-openssh-connections/

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

13 failles de sécurité critiques corrigées du côté de MDM

- Ivanti **M**obile **D**evice **M**anagement (MDM)
  - Composant WLAvalancheService
- Failles critiques
  - 9 vulnérabilités de type RCE
  - DDoS + contournement de la politique de sécurité
- Toutes les versions < 6.4.2.313 sont concernées

https://www.bleepingcomputer.com/news/security/ivanti-releases-patches-for-13-critical-avalanche-rce-flaws/

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

Désactiver l’intégration avec les BDD SQL sur 3CX

- Recommandation de l’entreprise
  - Aucune faille rendue publique, juste une suspicion
- 0.25% des utilisateurs seraient concernaient par cette faille potentielle
  - BDD MongoDB, MSSQL, MySQL & PostgreSQL
- Versions affectées :
  - 18
  - 20 (future version majeure en cours de finalisation)
- Documentée par 3CX : https://www.3cx.com/blog/news/sql-database-integration/

  https://www.securityweek.com/3cx-urges-customers-to-disable-integration-due-to-potential-vulnerability/

Failles / Bulletins / Advisories
Réseau (principales failles)

Centreon, multiples vulnérabilités exploitables à distance

- Vulnérabilités venant d'un pentest
- Peu de détails, pas de CVE (pour l'instant)

  `<< If [...] exposed on Internet [...]` **`high likelihood`** `of being exploited [...]` **`severe impact`** `[...]` **`high risk`** `>>`

  https://support.centreon.com/hc/en-us/articles/21413079841809-Security-bulletin-for-Centreon-Web

Failles / Bulletins / Advisories
Smartphones (principales failles)

Attaque AutoSpill sur Android (sans injection de JS)

- Abuse la fonction de remplissage automatique des gestionnaires de mots de passe
  - Permettant de voler les identifications stockés dans ces derniers
- Comment ?
  - En implémentant des webviews “corrompues” via une une application malveillante
  - Ex: (fausse) page de connexion Instagram <> auto-fill <> leak des creds
- Presque tous les gestionnaires sont vulnérables…
  - ❌**1Password** 7.9.4 (travail en cours)
  - ❌**LastPass** 5.11.0.9519
  - ❌**Enpass** 6.8.2.666
  - ❌**Keeper** 16.4.3.1048
  - ❌**Keepass2Android** 1.09c-r0
  - ☑**Google Smart Lock** 13.30.8.26
  - ☑**DashLane** 6.2221.3,
  - **Bitwarden** n’a pas été évalué ???

https://www.documentcloud.org/documents/24202397-eu-23-gangwal-autospill-zero-effort-credential-stealing

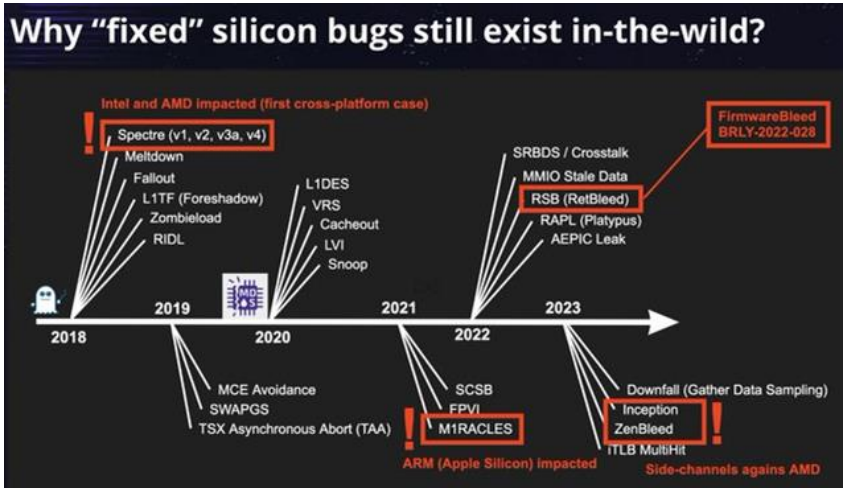
Failles / Bulletins / Advisories
Matériel

Revue des vulnérabilités matériel type “Spectre”

- Présenté à la LabsCon 2023

  https://twitter.com/matrosov/status/1740843192185164027

  https://www.youtube.com/watch?v=2Oksc5EejlY



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Pypi : infection (encore) **de la chaîne d'approvisionnement** (supply-chain attack)

- 116 malwares trouvés impactant les systèmes Windows & Linux
  - Disponible sur le dépôt PyPi (paquets Python libres)
  - Dont des variantes d'info-stealer type W4SP Stealer
- 10k téléchargements estimés depuis mai 2023 💀💀💀
- 3 techniques utilisées pour introduire du code malveillant dans les packages légitimes
  - N°1 : créer un fichier *test.py*
  - N°2 : intégration de PowerShell dans *setup.py*
  - N°3 : incorporer le code dans *__init__.py*

https://thehackernews.com/2023/12/116-malware-packages-found-on-pypi.html

Piratages, Malwares, spam, fraudes et DDoS
Piratages

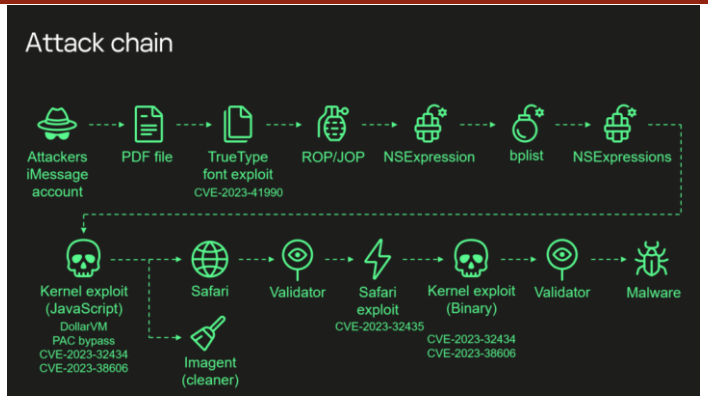
Piratage de MongoDB SaaS

- Accès aux informations concernant les clients, pas les données
- Attaque par harponnage (*spear phishing*) sur des salariés
  - Accès à l'outil de support aux client

https://next.ink/120689/mongodb-piratee-des-donnees-de-clients-dans-la-nature/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Triangulation, la suite (cf. revue du 13 Juin 2023)



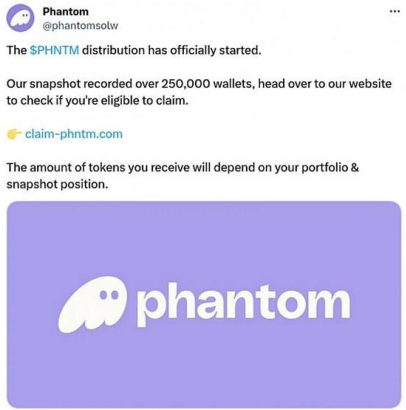
- Rappels :
  - Opération offensive ciblant Kaspersky de 2019 à 2023
    - Mais aussi des employés d'ambassade, politiques…
  - Opération unique, sans TTP déjà connu
  - FSB << c'est une opé américaine >>
- Mises à jour :
  - Exploitation de **4** vulnérabilités 0-days
    - CVE-2023-32434, CVE-2023-32435, CVE-2023-38606 et CVE-2023-41990
  - Premier accès par iMessage avec une vuln sur les polices de caractères (CVE-2023-41990)
    - Fonctionnalité visée spécifique à Apple (non documentée)
  - Chaîne d'exploitation très avancée
    - Utilisation d'une vuln Safari pour effacer ses traces et ensuite élever ses privilèges dans un autre processus
    - Rétro conception logicielle et matérielle TRES avancées (MMIO, fonctionnalité cachée)
  - Chaine non persistante

https://next.ink/121653/triangulation-kaspersky-victime-dune-longue-campagne-despionnage-hautement-sophistiquee/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Impact d'un compte X (Twitter) compromis...

- Compte de Mandiant (entreprise spécialisée dans la cyber)
  - + 124k abonnés
- Mot de passe ayant probablement fuité
- Compte renommé @mandiant → @phantomsolw
  - Servant à faire la promotion d'un faux site web usurpant l'identité du service Phantom
  - Promettant de distribuer gratuitement des jetons $PHNTM (via airdrop)
- But ? Vider le portefeuille de crypto d'un maximum de user
  - Heureusement, Phantom est intervenu rapidement
  - Mandiant a récupéré son compte (et changé son mot de passe) 😉



Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage chez Orange Espagne

- Surnommé “Snow”
- Compte RIPE NCC compromis
  - RIPE NCC : Réseaux IP Européens - Network Coordination Centre
  - Info-stealer permettant d’obtenir le mot de passe … **ripeadmin** 👏
  - Aucune MFA mise en place
- Trafic BGP détourné

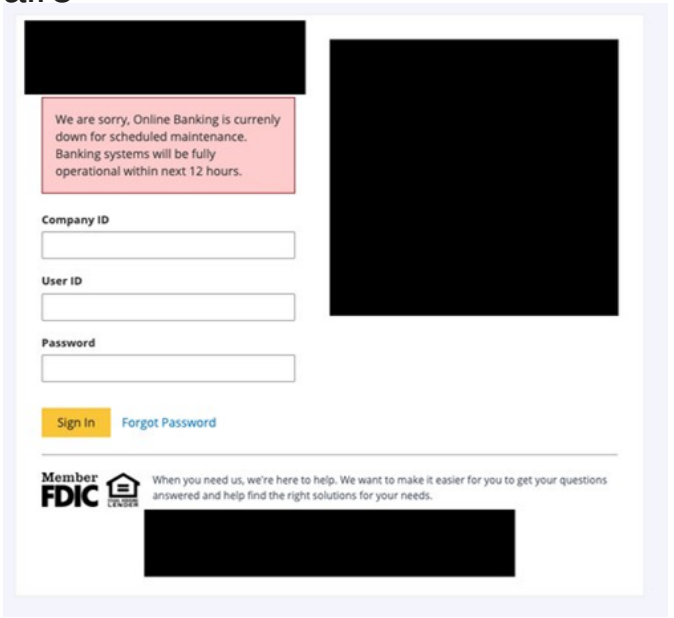
https://www.bfmtv.com/tech/actualites/telecoms/comment-un-mot-de-passe-faible-a-ruine-le-reseau-mobile-d-orange-en-espagne_AV-202401050469.html

Piratages, Malwares, spam, fraudes et DDoS
Malware

Info-stealer s’appuyant sur une “man-in-the-browser”

- Campagne lancée depuis mars 2023
  - Infection > **DanaBot**
  - Déjà 50k victimes à son actif (40 banques différentes)
- Injection de code JS sur la page de connexion au site bancaire
  - Intercepte les infos de connexion en temps réel
  - Vole les codes à usage unique (MFA)
  - Envoie les infos à un C2
  - Capable de s’auto-supprimer
  - Dissuade l’utilisateur de se connecter ---------->
- N’est pas compatible avec toutes les banques, “lol”

https://www.theregister.com/2023/12/20/credentialstealing_malware_infects_50k_banking/



Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Clap de fin pour le groupe de BlackCat

- Site vitrine mis hors ligne
- FBI accompagné par Europol et par d'autres services de police
  - Danemark, Allemagne, Royaume-Uni, Pays-Bas, Australie, Espagne et Autriche
  - Maintien sur l'infra du groupe pendant plusieurs mois
- 500 victimes ont pu restaurer leurs systèmes
  - Via un outil maison développé par le FBI
  - ~ 68 millions de $ économisés
- 946 paires de clés publiques / privés associés à des sites Tor ont été récupérées

https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant (rapport justice.gov)

https://www.it-connect.fr/le-fbi-met-a-larret-linfrastructure-du-ransomware-blackcat-et-dechiffre-les-donnees-de-500-victimes/

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Black Basta Buster vs Black Basta

- Outil de déchiffrement développé par SRLabs
  - Exploite une faille de sécurité dans l'algorithme de chiffrement
- Déchiffrement possible des données pour les victimes
  - Celles ayant eu leurs données chiffrées entre 11/2022 et 12/2023 = 153 victimes
  - Toutes les données ne sont pas récupérables
    - ❌ < 5000 octets
    - 5000 octets <= ❓ <= 1 Go
    - ☑ > 1 Go (mais les 5000 premiers octets seront perdus)
  - Un fichier par un fichier (c'est déjà bien)
- Le groupe a déjà fait le nécessaire pour palier à cette faiblesse

https://github.com/srlabs/black-basta-buster (outil)

https://www.darkreading.com/cloud-security/black-basta-buster-exploits-ransomware-bug-file-recovery

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Coaxis victime de LockBit 3.0

- Aucune communication sur le “comment” de l’intrusion
  - Maybe Citrix ? (cf. revue du 12/09/2023)
- Ensemble du SI de nouveau opérationnel
- Leak disponible sur le site vitrine de LockBit 3.0 le 09/01/2024 à 19h CET
  - Ne contiendrait pas de données clientes / personnelles
  - Aucune information sur la taille et le type de données

https://www.lemagit.fr/actualites/366564634/Coaxis-la-cyberattaque-revendiquee-sur-la-vitrine-de-LockBit-30

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

Retour sur le ransomware chez Norton Healthcare

- Alphv (BlackCat)
- Données volées de 2.5 millions de personnes
  - Noms, coordonnées, n° sécurité sociale, dates de naissance, n° permis de conduire, etc.
- Et également…
  - Informations de santé, informations d'assurance, anciens patients, etc.
- Attaque réalisée en **mai 2023**
  - Début des notifications des victimes **début décembre**

https://www.theregister.com/2023/12/11/norton_healthcare_ransomware/

https://www.hipaajournal.com/norton-healthcare-data-breach/

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

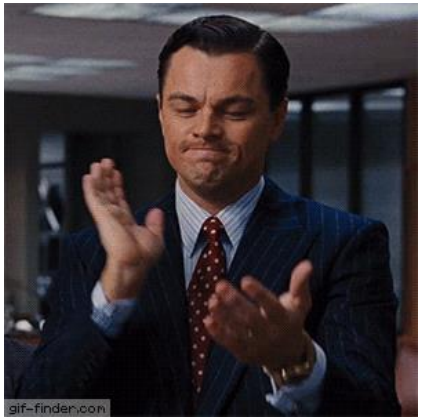
Fuite de données chez 23andMe

- Aucune violation des systèmes internes
  - Les accès à 14k comptes ont été obtenus via du bourrage
  - + 7 millions d'accès obtenus via la fonctionnalité optionnelle de partage ADN
- La société nie toute responsabilité
  - Les utilisateurs responsables ???
  - MFA disponible, mais mesure insuffisante
    - Aucune politique de mot de passe
    - Aucune notification envoyée à l'utilisateur lorsque la connexion est réalisée depuis un lieu inhabituel

https://www.darkreading.com/cyberattacks-data-breaches/23andme-negligent-users-at-fault-breach-7m-records

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

Résultats sur l'opération HAECHI IV



- 3 500 cybercriminelles arrêtés et $300 millions saisis
- Opération déroulée entre 07/2023 et 12/2023
  - Objectif : arrêter les personnes impliquées dans des activités de :
    - Vishing (voice phishing)
    - Romance scams (ou love scams)
    - Sextorsion
    - Fraude à l'investissement
    - Compromission de boites mails
  - Gérée par Interpol
  - Financée par la Corée du Sud
  - 35 pays ont collaborés : USA, UK, etc. (pas la France)
- +260% d'arrestations par rapport à HAECHI III (06/2022 - 11/2022)

https://www.interpol.int/en/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation (rapport d'Interpol)

https://www.it-connect.fr/interpol-saisit-300-millions-de-dollars-et-arrete-3-500-cybercriminels/

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

Blue Team CyberChef permet de valider les Yara

- Outils open source du GCHQ
  - Accessible ici https://gchq.github.io/CyberChef/

https://twitter.com/h_miser/status/1743684758310170880

Blue Team Les IoC les plus détaillés que vous ne verrez jamais 😂

- Fournis avec amour par Blackberry 🤪

https://blogs.blackberry.com/en/2023/11/aeroblade-on-the-hunt-targeting-us-aerospace-industry

Both lure documents were named "**[redacted].docx**."
The final payload is a reverse shell.

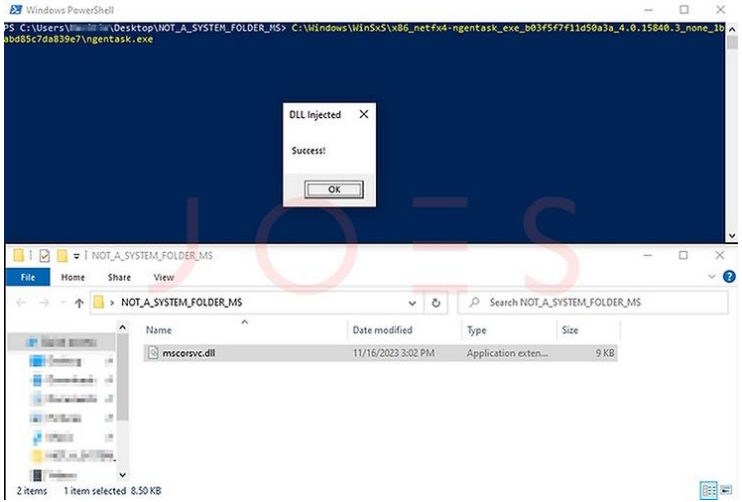
d [redacted].docx is delivered via email spear-phishing, which, v
download a second stage file called "**[redacted].dotm**". This file
cted[.]redacted[.]com" over port 443

IP	Domain Name
[redacted].217	hxxp://[redacted].217/[redacted][.]dotm hxxp://[redacted].217/[redacted]
[redacted].195	redacted.redacted.com
[redacted].165	redacted.redacted.com

Red Team Variante de la DLL hijacking

- Tous les Windows sont vulnérables 🎯
- Cible les binaires dans *C:\Windows\WinSxS*
  - Windows Component Store : fichiers nécessaires à la restauration du système
- Binaire lancé depuis un répertoire contrôlé + DLL malveillante = exécution de code ☠️

https://www.securityjoes.com/post/hide-and-seek-in-windows-closet-unmasking-the-winsxs-hijacking-hideout



Red Team Contournement d'ASLR sans fuite d'information

- Nécessite tout de même:
  - Une fuite mémoire 😉
    - Memory leak != Information leak
    - Memory leak == oups, j'ai oublié de "dé-aouller" une zone mémoire
  - Un gadget spécifique pour réaliser du "spaying"
  - Un Oracle

https://github.com/nick0ve/how-to-bypass-aslr-on-linux-x86_64

Business et Politique

Business
Monde

Acquisition d'Imperva par Thales

- 9 milliards
- Imperva : société éditrice de logiciels et de services cyber
  - 9ème acquisition du groupe dans le domaine en 9 ans !
- But ?
  - Acquérir de nouveaux produits "home-made" : WAF, anti DDoS, CDN, RASP, etc.

`<< [...] it marks a new step in the expansion of our global cybersecurity capabilities >>`

https://www.thalesgroup.com/en/worldwide/security/press_release/thales-completes-acquisition-imperva-creating-global-leader

Droit / Juridique / Politique
Juridique

FISA prolongée

- La section 702 de la loi FISA est prolongée jusqu'en avril 2024
  - « **F**oreign **I**ntelligence **S**urveillance **A**ct »
  - Collecte et accès en masse aux données des Européens (mails, appels tel, réseau sociaux…)

https://www.01net.com/actualites/philippe-latombe-la-loi-fisa-cest-une-bombinette-qui-pourrait-faire-voler-en-eclat-notre-souverainete-numerique.html

Signature electronique invalidée ?

- Si les conditions pour garantir l'opposabilité, ne sont pas réunie
- Il faut prouver le lien entre la signature et le signataire
  - MFA, validation de l'identité…

https://www.usine-digitale.fr/article/absence-de-fiabilite-de-la-signature-electronique.N2204828

Droit / Juridique / Politique
Juridique

Condamnation du hackeur de GTA VI

- Membre du groupe Lapsu$ (Piratage de Nvidia, Rockstar Games, Uber, Microsoft, Samsung…)
- Arion Kurtaj, 18 ans, autiste, condamné à une hospitalisation sans limite de durée

https://www.lemonde.fr/pixels/article/2023/08/23/cybercriminalite-la-justice-britannique-relie-deux-adolescents-aux-attaques-attribuees-au-groupe-lapsus_6186324_4408996.html

L'influenceur Instagram était un scammer + brouteur + délinquants

- L'influenceur Hushpuppi (Ramon Abbas) était en réalité un délinquant
  - Arnaques au sentiment (scam nigérian)
  - Piratages de comptes mails (fausses factures, changement de RIB…)
  - Piratages de banques en ligne
  - Usurpation de banque
  - Panique à Malte en 2019 suite au blanchiment de $13m de hackeurs nord-coréens
- Condamné à 11 ans de prison aux USA

https://www.bbc.com/afrique/articles/ck7e0g2np42o

https://www.youtube.com/watch?v=RC0usdMcKGQ

Conférences

Conférences

À venir

- JSSI, 12 mars 2024 à Paris
  - Thème : « Intelligence artificielle et [in]sécurité »
- CoRIIN, 26 mars 2024 à Lille
  - En parallèle du FIC
- FIC, 26 au 28 mars 2024 à Lille
- BotConf, 24 au 26 avril 2024 à Nice #BoufConf / #BouffeConf
- SSTIC, 05 au 07 juin 2024 à Rennes
- LeHack « Compile », 05 au 07 juillet 2024 à Paris (20ème édition !)

Divers / Trolls velus

Divers / Trolls velus

Problème pour vous connecter en Wi-Fi sur votre Windows 11 ? Encore un bug ?

- Affecte les Windows 11 22H2 et 23H2 ayant reçu la maj KB5033375
- Bug rendant impossible la connexion à certains réseaux Wi-FI
  - Ceux utilisant l'authentification 802.1x
  - Ce n'est donc pas un bug lié à l'option fast roaming (IEE 802.11r) comme annoncé auparavant !
- Patch via le service KIR (Know Issue Rollback)
  - Ou via le package fourni par Microsoft : "Windows 11 22H2 KB5032288 231029_032011 Known Issue Rollback" https://download.microsoft.com/download/3/d/4/3d4cf819-692d-48cd-a118-49db712250c9/Windows%2011%2022H2%20KB5032288%20231029_032011%20Known%20Issue%20Rollback.msi
- Attention Microsoft avec vos bugs gênants…
  - Bug des imprimantes renommées en "HP LaserJet M101-M106" #OSSIR_12/12/2023
    - Outil pour patcher ce bug : https://www.microsoft.com/en-us/download/details.aspx?id=105763

https://www.it-connect.fr/windows-11-microsoft-a-resolu-letrange-probleme-de-connexion-wi-fi-voici-la-solution/

Divers / Trolls velus

Plans de Microsoft pour sécuriser le spooler d'impression

- Service connu pour être très vulnérable…

`<< Les bugs d'impression ont joué un rôle dans Stuxnet et Print Nightmare, et représentent **9%** de tous les cas de Windows signalés au MSRC >>`

- **W**indows **P**rotected Print **M**ode \o/
  - Présent dans les derniers builds de Windows à des fins de tests
  - Éliminerait 50% des vulns connus sur le service
  - Qu'apporte-t-il ?
    - Le service ne se lance plus en tant que SYSTEM
    - Rendu XPS effectué en tant qu'utilisateur (vs SYSTEM avant)
    - WPP annoncera si le trafic entre le device Windows et l'imprimante est chiffré ou non
    - Blocage des pilotes et des binaires tiers
    - "Impossible" de charger une DLL malveillante depuis le port d'imprimante
- Microsoft va également activer d'autres protections
  - Atténuation matérielle (pour prévenir du ROP), désactivation de la création de processus enfant, redirection guard ("path redirection" ❌) & arbitrary code guard (empêcher la génération de code dynamique au sein d'un processus)

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/a-new-modern-and-secure-print-experience-from-windows/ba-p/4002645

Divers / Trolls velus

Fin des licences perpétuelles chez VMware

- Officialisé par Broadcom
  - Qui a racheté VMware en novembre pour 61 milliards de dollars
- Au revoir les licences, bonjour les abonnements !
  - Encore des licences actives ? Elles seront toujours fonctionnelles mais ne seront pas par renouvelées
- 2 produits principaux :
  - VMware Cloud Foundation (environnements de grande taille)
  - VMware vSphere Foundation (environnements de petite et moyenne taille)
- Le reste (vSphere Standard & Essentials Plus) ?
  - Toujours commercialisées

https://www.lemondeinformatique.fr/actualites/lire-broadcom-elimine-les-licences-perpetuelles-de-vmware-92419.html

Divers / Trolls velus

Jean-Michel Mytho est de retour…

- Après ses mensonges sur Pegasus, Android, Citizenlab… (cf. revue du 12/07/2022)
- Après l'ouverture d'une enquête par le comité de revue de son université (cf. revue du 12/07/2022)
- La **Police Nationale** du **Rwanda** fait un communiqué officiel :
  - << RNP HAS NOT HIRED JONATHAN SCOTT >>

    https://twitter.com/rwandapolice/status/1743767506982973608

    https://twitter.com/TheMiladGroup/status/1743836546728407395 (J.S. est le fondateur de Milad)

Le cabinet juridique en charge des fuites de données…

- À vu ses données fuiter

  https://techcrunch.com/2024/01/04/orrick-law-firm-data-breach/

Divers / Trolls velus

Moi aussi je veux accéder à votre caméra !

- Accès aux caméras un peu trop … verbeux
  - Via Cloud UniFi
  - Et également aux points d'accès Wi-Fi et aux routeurs !
- "Mauvaise configuration appliquée lors d'une mise à niveau de l'infrastructure Cloud d'UniFi"
  - Un groupe A (1177 comptes) ayant accès aux équipements d'un groupe B (1216 comptes)
- Entre 6h47 et 15h45 UTC = 9 heures de libre accès 👀

https://www.it-connect.fr/des-utilisateurs-dubiquiti-ont-pu-acceder-aux-routeurs-et-cameras-dautres-utilisateurs/

Divers / Trolls velus

La Russie utilise les caméras à Kiev pour faire de la reconnaissance

- Information fournie par les services ukrainiens sur Telegram
- Caméras initialement centrées sur des parkings
  - Fonctionnant avec un firmware russe…
  - Redirigées vers des endroits stratégiques (forces anti-aériennes)
- Flux vidéo également diffusés sur YouTube 😳

https://www.numerama.com/cyberguerre/1599086-larmee-russe-a-pirate-des-cameras-en-ukraine-pour-envoyer-ses-missiles-sur-les-villes.html

Merci pour votre confiance 🙏

Dernière revue d'actu pour Vlad

11 février 2014 - 9 janvier 2024

10 ans 😱

(cette date de fin, pour un chiffre rond, est un pur hasard… si si !)

À nouveau, nos meilleurs voeux pour **2024** !

Et maintenant ?

Prochaine réunion ?

RDV le mardi **13 février**

FIN

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous