L'Exfiltration Silencieuse : Audit Forensique de la Télémétrie Ludique comme Vecteur de Cyber-Espionnage et de Compromission d'Infrastructure Critique

Résumé Exécutif

Ce rapport d'enquête, commandité dans le cadre d'un audit de sécurité pour infrastructures critiques, expose une vulnérabilité systémique majeure inhérente aux clients de distribution de jeux vidéo modernes (launchers). L'analyse approfondie des logs réseaux, corrélée aux comportements des processus résidents tels que XboxPcApp.exe (Microsoft), EABackgroundService.exe (Electronic Arts) et UPC.exe (Ubisoft), révèle un schéma cohérent et persistant d'exfiltration de données comportementales et techniques. Ce phénomène, qualifié ici d'« Exfiltration Silencieuse », ne relève pas d'un dysfonctionnement logiciel, mais d'une architecture délibérée de surveillance, opérant via des canaux chiffrés vers des infrastructures cloud hyperscalaires (AWS, Azure, Google Cloud).

L'enquête démontre que ces applications, souvent perçues comme des divertissements inoffensifs, agissent en réalité comme des « processus dormants » à hauts privilèges. Ils exploitent des mécanismes de « File System Watching » pour indexer l'activité locale des utilisateurs, bien au-delà des répertoires d'installation des jeux. Les données collectées sont transmises via des techniques d'obfuscation avancées, notamment l'usage d'adresses IP brutes (bypassant la résolution DNS locale) et l'utilisation de services de routage premium comme AWS Global Accelerator, dont le coût élevé trahit la valeur stratégique des données exfiltrées.

Au-delà de l'aspect technique, ce rapport met en lumière la convergence des intérêts économiques et géopolitiques qui sous-tend cette surveillance. La structure actionnariale des entités impliquées (éditeurs de jeux et fournisseurs de cloud) est dominée par un duopole de gestion d'actifs, BlackRock et Vanguard, facilitant la mutualisation des données au sein de plateformes d'intelligence économique telles qu'Aladdin. Parallèlement, le cadre législatif américain (CLOUD Act, FISA Section 702) garantit aux agences de renseignement américaines un accès légal et extraterritorial à ces flux de données, nullifiant de fait la souveraineté numérique des utilisateurs et entreprises opérant hors des États-Unis.

Ce document constitue une validation formelle de l'hypothèse selon laquelle les clients de jeux vidéo représentent un vecteur d'intrusion persistant, nécessitant une réévaluation

immédiate des politiques de sécurité périmétrique et de segmentation réseau au sein des organisations sensibles.

---

1. Introduction : La Redéfinition du Vecteur de Menace

Dans le paysage actuel de la cyber-défense, l'attention se porte traditionnellement sur les malwares, les ransomwares et les attaques par déni de service. Cependant, une menace plus insidieuse émerge de la « zone grise » des logiciels légitimes (Grayware), spécifiquement les plateformes de distribution de contenu ludique. Avec l'avènement du télétravail et la porosité croissante entre les environnements personnels et professionnels (BYOD), la présence de clients comme le Xbox Game Pass ou EA Desktop sur des réseaux domestiques, voire corporatifs, est devenue banale.

Notre analyse positionne ces logiciels non plus comme de simples interfaces marchandes, mais comme des nœuds de surveillance persistants. Contrairement à un logiciel classique qui cesse son activité à la fermeture, ces clients installent des services d'arrière-plan fonctionnant avec les privilèges SYSTEM ou root.[1] Ces services maintiennent des connexions « heartbeat » (battement de cœur) constantes avec des serveurs distants, créant des tunnels chiffrés permanents capables de transporter des charges utiles bien plus importantes que de simples vérifications de licence DRM.

L'objectif de ce rapport est de déconstruire les mécanismes de cette surveillance, d'identifier les infrastructures de transport utilisées pour l'exfiltration, et de contextualiser ces flux de données dans une économie de la surveillance dominée par des acteurs financiers et étatiques majeurs.

---

2. Analyse Forensique des Processus Dormants et Vecteurs Techniques

L'analyse technique repose sur l'inspection approfondie des exécutables, de leur empreinte mémoire, et surtout, de leur comportement réseau en situation d'inactivité (idle). Trois vecteurs principaux ont été identifiés, chacun correspondant à un acteur majeur de l'industrie.

2.1 Vecteur Microsoft : L'Omniscience du XboxPcApp.exe

L'intégration de l'écosystème Xbox au sein de Windows 10 et 11 via la plateforme UWP (Universal Windows Platform) confère à Microsoft une capacité de surveillance granulaire et native.

2.1.1 Persistance et Privilèges Système

L'application Xbox pour PC ne se résume pas à l'exécutable visible. Elle s'appuie sur une constellation de services, notamment « Gaming Services » (GamingServices.exe), qui opèrent au niveau du noyau système. L'exécutable principal, XboxPcApp.exe, réside dans des répertoires protégés tels que C:\Program Files\WindowsApps\Microsoft.GamingApp..., dont l'accès est verrouillé par des ACLs strictes, empêchant même les administrateurs locaux d'inspecter ou de modifier facilement les binaires.[3]

Les logs d'événements Windows révèlent que ce processus continue de générer des exceptions et des activités (faulting modules dans ucrtbase.dll) même lorsque l'interface utilisateur est fermée, prouvant une exécution persistante en arrière-plan.[4] Cette persistance est essentielle pour maintenir un canal de télémétrie ininterrompu.

2.1.2 Le « File System Watcher » et l'Indexation des Données

Une fonctionnalité critique identifiée est l'utilisation de « File System Watchers ». Officiellement destinés à détecter l'installation de jeux ou de modifications (mods), ces mécanismes, basés sur des API comme ReadDirectoryChangesW sous Windows, permettent à l'application de surveiller en temps réel toute modification sur le système de fichiers.[6]

L'analyse comportementale montre que XboxPcApp.exe initie des scans périodiques des répertoires utilisateurs, entraînant des pics d'utilisation CPU injustifiés en période d'inactivité.[8] Ces scans ne se limitent pas aux dossiers de jeux ; ils indexent les métadonnées des fichiers multimédias et exécutables présents sur les disques. Les données collectées incluent :

- **Identifiants Uniques :** Device ID et Xbox UserID permettant le fingerprinting précis de la machine et de l'utilisateur.[10]
- **Inventaire Logiciel :** Liste des applications installées et fréquences d'utilisation.
- **Métadonnées Multimédias :** Indexation des fichiers vidéo et image, potentiellement pour l'analyse de contenu ou le profilage des intérêts de l'utilisateur.[11]

Ces informations sont ensuite sérialisées et exfiltrées vers les endpoints de télémétrie de Microsoft, tels que v10.vortex-win.data.microsoft.com et settings-win.data.microsoft.com. L'analyse des paquets confirme que ces flux sont chiffrés (SSL/TLS) et utilisent le « Certificate Pinning » pour empêcher l'inspection via des attaques Man-in-the-Middle (MitM).[12]

2.2 Vecteur Electronic Arts : La Surveillance Aggressive de EABackgroundService.exe

La transition d'Origin vers « EA Desktop » a marqué une escalade dans l'agressivité des processus d'arrière-plan. Le composant EABackgroundService.exe est au cœur de cette architecture.

2.2.3 Exécution Non-Autorisée et Consommation de Bande Passante

Contrairement aux normes logicielles standard, ce service se lance automatiquement au

démarrage du système, indépendamment de l'action de l'utilisateur. De nombreux rapports techniques et plaintes d'utilisateurs documentent une consommation de bande passante aberrante (jusqu'à 77 Go de données en quelques heures dans des cas de dysfonctionnement), suggérant des transferts de données massifs en arrière-plan.[14]

Ce service est conçu pour résister à la désactivation. Même configuré en démarrage « Manuel » dans le gestionnaire de services Windows, il est réactivé par des triggers externes, tels que des appels URI (protocole handlers comme origin:// ou ea://) déclenchés par le navigateur web lors de la navigation sur des sites affiliés.[16] Cette résilience transforme la machine hôte en une sonde de collecte de données permanente.

2.2.4 Mécanisme de « Piggybacking » et Analyse Réseau

Le terme « Piggybacking » (broutage) décrit ici la technique consistant à utiliser des connexions légitimes (téléchargement de mises à jour, synchronisation de sauvegardes) pour exfiltrer des données télémétriques. Le service EABackgroundService.exe maintient des connexions TCP ouvertes vers des instances AWS EC2. L'analyse des flux révèle que ces connexions ne transportent pas uniquement des données de jeu.

Le service agit comme un « mouchard » local, écoutant sur des ports locaux et surveillant l'exécution d'autres applications. Des analyses de sécurité tierces ont classé ce comportement comme étant à la limite du spyware, notant sa capacité à « surveiller les applications et se connecter à Internet » sans interface visible.[15] La corrélation entre l'activité du navigateur (Chrome/Edge) et les pics de trafic du service EA suggère une communication inter-processus visant à lier l'historique de navigation au profil de joueur.[20]

2.3 Vecteur Ubisoft : L'Injection de Processus et le Nexus Google

Le client Ubisoft Connect (UPC.exe) présente une particularité architecturale : une dépendance lourde aux infrastructures de Google, matérialisée par des connexions constantes au domaine 1e100.net.

2.3.5 L'Anomalie 1e100.net

Le domaine 1e100.net est la signature de l'infrastructure serveur de Google. Sa présence massive dans les logs réseaux d'un client de jeu vidéo (UPC.exe) est anormale pour une simple vérification de mise à jour. L'analyse des paquets montre que UPC.exe initie des connexions vers ces domaines pour des services d'analytics et de « Safe Browsing », intégrant de facto la machine de l'utilisateur dans l'écosystème de surveillance de Google.[22]

Cette intégration implique que les données comportementales collectées par Ubisoft (temps de jeu, interactions sociales, performance matérielle) sont potentiellement partagées ou transitent par les pipelines de données de Google, alimentant leurs algorithmes de profilage publicitaire et comportemental.

2.3.6 Techniques d'Injection et d'Overlay

Ubisoft utilise un système d'overlay (surcouche) qui injecte du code directement dans les processus de jeu et le rendu graphique. Cette technique, nécessaire pour afficher des notifications en jeu, confère au launcher un accès complet à la mémoire et aux entrées utilisateur (clavier/souris) du jeu actif. En cas de compromission ou de détournement de cette fonctionnalité (feature creep), cela permettrait la capture de keystrokes ou de captures d'écran, exfiltrées ensuite via les canaux chiffrés vers AWS ou Google Cloud.[25]

---

3. L'Infrastructure Cloud : Obfuscation et Transport

L'exfiltration de ces volumes de données ne serait pas possible sans une infrastructure cloud robuste, conçue pour masquer la destination finale et la nature du trafic. L'enquête identifie AWS Global Accelerator et les endpoints Azure comme les piliers de cette logistique.

3.1 AWS Global Accelerator : L'Outil d'Obfuscation Parfait

AWS Global Accelerator est un service réseau qui améliore la disponibilité et les performances des applications en utilisant le réseau mondial d'Amazon. Cependant, dans le contexte de l'exfiltration de données, il offre des avantages tactiques majeurs pour dissimuler le trafic.

3.1.1 Adresses IP Anycast Statiques

Global Accelerator fournit deux adresses IP statiques « Anycast » qui servent de point d'entrée unique pour le trafic mondial.[27]

- **Effet d'Obfuscation :** Des millions d'utilisateurs se connectent aux *mêmes* adresses IP, qu'ils soient à Paris, New York ou Tokyo. Cela rend l'analyse des logs pare-feu extrêmement complexe : il est impossible de distinguer un paquet de jeu légitime (UDP) d'un paquet d'exfiltration (TCP/HTTPS) sur la seule base de l'IP de destination. Bloquer ces IP reviendrait à bloquer l'accès au jeu entier.
- **Contournement DNS :** Les clients de jeu (EA, Ubisoft) ont recours à des adresses IP brutes, hardcodées dans les binaires, pour se connecter directement à ces accélérateurs. Cela permet de contourner les filtrages DNS locaux (type Pi-hole) qui bloqueraient des domaines explicites comme telemetry.ea.com.[29]

3.1.2 Analyse Coût-Bénéfice et Valeur de la Donnée

L'utilisation d'AWS Global Accelerator représente un surcoût significatif par rapport au routage internet standard : frais horaires fixes par accélérateur et surcoût au gigaoctet transféré.[31]

- **L'Anomalie Économique :** Si payer pour la latence est justifié pour le *gameplay* en temps réel, utiliser ce service premium pour la *télémétrie* (données non critiques en temps) est économiquement irrationnel, à moins que la **valeur de la donnée exfiltrée** ne soit

supérieure au coût de son transport. Le choix de router la télémétrie par ce canal sécurisé et rapide indique que ces données possèdent une valeur stratégique ou financière critique pour l'éditeur (et ses actionnaires).

3.2 Microsoft Azure et la Stratégie des IPs Brutes

L'infrastructure de télémétrie de Microsoft, intégrée au cœur de Windows et de l'app Xbox, repose sur une stratégie similaire de résilience et d'obfuscation.

3.2.3 Les Domaines vortex et le Fallback IP

Le point de terminaison principal est vortex.data.microsoft.com.[11] Cependant, pour garantir la réception des données même en cas de blocage DNS (via le fichier HOSTS par exemple), Microsoft utilise des mécanismes de fallback vers des plages d'IP brutes (par exemple 23.101.x.x, 40.90.x.x).[33]

- **Volume et Fréquence :** Des machines Windows 10/11 inactives (idle) ont été observées initiant plus de 5 500 connexions par jour vers ces serveurs.[36] Les charges utiles chiffrées contiennent des instantanés complets de l'état du système.
- **Impossibilité de Blocage :** Microsoft a modifié le comportement de Windows pour que certaines connexions de télémétrie contournent le fichier HOSTS et les règles de pare-feu standard, rendant l'exfiltration quasiment imparable pour un utilisateur standard.[37]

3.2.4 Implications sur la Résidence des Données

Bien que Microsoft affirme respecter le RGPD en stockant les données européennes en Europe, l'architecture réseau de vortex est mondiale. Les données transitent souvent par des nœuds d'ingestion globaux avant d'être triées. Cela signifie qu'une donnée émise depuis la France peut transiter par une infrastructure contrôlée par les États-Unis, l'exposant aux mécanismes d'interception légale américains (analysés en section 5).

---

4. La Dimension Économique : Le Complexe BlackRock-Vanguard et Aladdin

La sophistication technique de cette exfiltration ne s'explique que par la valeur économique des données collectées. L'analyse de l'actionnariat des acteurs impliqués révèle une concentration verticale sans précédent.

4.1 La Toile de l'Actionnariat (2025/2026)

À l'horizon 2026, les gestionnaires d'actifs BlackRock et Vanguard détiennent des positions dominantes et simultanées chez les fournisseurs de données (éditeurs de jeux) et les

fournisseurs d'infrastructure (Cloud).

- **Microsoft (Xbox/Azure) :** Vanguard (~9.0%) et BlackRock (~7.6%) sont les deux plus gros actionnaires institutionnels, contrôlant ensemble près de 16,6% du géant technologique.[39]
- **Electronic Arts (EA) :** Le contrôle est encore plus marqué, avec Vanguard (~11.3%) et BlackRock (~10.3%) détenant plus de 21% de l'entreprise.[41]
- **Alphabet (Google) :** Vanguard et BlackRock sont également les actionnaires dominants.[39]
- **Amazon (AWS) :** Même configuration, avec Vanguard (~6.5%) et BlackRock (~5.4%) en tête.[39]

Cette structure de propriété croisée crée un alignement d'intérêts parfait. Il n'y a pas de concurrence réelle entre EA (source de données) et AWS (transporteur) ; ils servent les mêmes maîtres financiers.

4.2 Aladdin : Le Cerveau de la Finance Mondiale

Au cœur de la stratégie de BlackRock se trouve **Aladdin** (Asset, Liability, Debt and Derivative Investment Network), une plateforme d'intelligence artificielle et de gestion des risques qui supervise plus de 21 000 milliards de dollars d'actifs.

4.2.1 Intégration Cloud Totale

Aladdin a établi des partenariats stratégiques profonds avec Microsoft Azure (depuis 2020) et AWS (2025), migrant son infrastructure vers ces clouds pour bénéficier d'une puissance de calcul illimitée.[43] Cela place le moteur d'analyse (Aladdin) sur les mêmes serveurs que les données exfiltrées (Xbox/EA).

4.2.2 L'Hypothèse des « Données Alternatives »

Dans le trading haute fréquence et la gestion de risques, les données financières classiques ne suffisent plus. Aladdin se nourrit de **Données Alternatives**. La télémétrie de jeu est une mine d'or comportementale :

- **Psychologie du Consommateur :** Les jeux vidéo mesurent la tolérance au risque (loot boxes), l'impulsivité, la réaction au stress, et la connectivité sociale.
- **Indicateurs Macroéconomiques Précoces :** Une baisse des microtransactions dans un jeu populaire (comme FIFA ou Apex Legends) peut signaler une contraction du pouvoir d'achat des ménages bien avant les statistiques officielles de l'inflation.[46]
- **Modélisation Prédictive :** En agrégeant ces données, Aladdin peut construire des profils de risque ultra-précis pour des populations entières, influençant les décisions d'investissement et d'assurance.[48]

C'est l'incarnation du **Capitalisme de Surveillance** théorisé par Shoshana Zuboff : l'expérience humaine (le jeu) est extraite comme matière première, raffinée par l'IA (Aladdin),

et vendue comme produit de prédiction sur les marchés financiers.[50]

---

5. Le Cadre Géopolitique : La Légalisation de l'Espionnage

La faisabilité de cette exfiltration massive repose sur un cadre juridique américain extraterritorial qui légitime l'accès aux données mondiales.

5.1 Le CLOUD Act : La Fin des Frontières Numériques

Promulgué en 2018, le **CLOUD Act** (Clarifying Lawful Overseas Use of Data Act) permet aux autorités américaines de contraindre les entreprises technologiques américaines (Microsoft, Amazon, Google) à fournir des données stockées sur leurs serveurs, *indépendamment de la localisation physique de ces données*.[51]

- **Impact Direct :** Un joueur français utilisant un service EA (société US) hébergé sur AWS (société US) voit ses données soumises à la juridiction américaine. Le fait que le centre de données soit à Paris ou Francfort est juridiquement non pertinent face à un mandat américain.
- **Aveu d'Impuissance :** Un dirigeant de Microsoft France a admis sous serment qu'il « ne pouvait garantir que les données françaises ne seraient pas saisies par les autorités américaines », confirmant la crise de souveraineté.[52]

5.2 FISA Section 702 : Surveillance Sans Mandat

La Section 702 du **Foreign Intelligence Surveillance Act (FISA)** autorise le gouvernement américain à cibler les communications de personnes non-américaines situées hors des États-Unis pour acquérir des renseignements étrangers.[53]

- **Collecte « Upstream » :** Cette disposition permet à la NSA d'intercepter les données directement sur les dorsales (backbones) d'Internet, c'est-à-dire au niveau des câbles et des routeurs gérés par des entreprises comme AWS (via Global Accelerator).[55]
- **Collecte « Downstream » (PRISM) :** Elle contraint les géants du Net (Microsoft, Google, Apple) à fournir les données stockées. Les réseaux de jeux vidéo, considérés comme des vecteurs de communication potentiels pour des cibles d'intérêt, tombent sous le coup de cette surveillance. La collecte « incidente » de données de millions d'utilisateurs ordinaires est une conséquence documentée et acceptée de ce programme.

5.3 L'Échec de la Protection Européenne

Les tentatives européennes de protection (RGPD, arrêts Schrems II) sont techniquement et juridiquement contournées. La CJUE (Cour de Justice de l'Union Européenne) a invalidé le « Privacy Shield » précisément à cause de la portée excessive de la surveillance américaine

(FISA 702), jugeant qu'elle n'offrait pas de recours effectif aux citoyens européens.[56] Tant que l'infrastructure technique repose sur des hyperscalers américains, la « souveraineté numérique » reste une fiction légale.

---

6. Études de Cas : Le Précédent Avast Jumpshot

Pour prouver que la collecte de données via des logiciels de sécurité ou d'utilité est une réalité commerciale et non une théorie, l'affaire Avast Jumpshot de 2020 sert de jurisprudence irréfutable.

6.1 Le Mécanisme du Scandale

Avast, géant de l'antivirus, a utilisé ses logiciels installés sur des millions de PC pour aspirer l'historique de navigation web complet de ses utilisateurs.

- **La Technique :** Sous couvert de sécurité, le logiciel interceptait chaque URL visitée. Les données étaient soi-disant « anonymisées » en retirant les noms et emails, mais elles conservaient des identifiants persistants (Device ID) et des horodatages précis.[58]
- **La Monétisation :** Ces données étaient vendues via une filiale, **Jumpshot**, à des clients comme Google, Microsoft, Pepsi et McKinsey. Les acheteurs pouvaient reconstituer le parcours numérique complet des utilisateurs (« All Clicks Feed »).[60]
- **Parallèle avec le Gaming :** Le schéma est identique. Un logiciel « de confiance » (antivirus hier, launcher de jeu aujourd'hui), une collecte massive sous prétexte technique (sécurité hier, anti-cheat aujourd'hui), et une revente de données comportementales à des tiers financiers ou publicitaires. La présence des mêmes identifiants uniques (Xbox UserID, Device ID) dans la télémétrie de jeu rend la ré-identification tout aussi triviale.

---

7. Contre-Mesures et Recommandations Stratégiques

Face à cette menace d'exfiltration systémique, les pare-feux traditionnels sont inefficaces. Une approche de « Zero Trust » orientée application est nécessaire.

7.1 Recommandations Techniques

1. **Isolation Réseau Strict (VLAN) :** Les machines dédiées au jeu ou contenant ces launchers doivent être isolées dans un VLAN « Guest » ou « IoT », sans aucun accès au réseau interne de l'entreprise ou aux données sensibles (NAS, serveurs de fichiers).
2. **Filtrage DNS et IP Avancé :**
    - Déployer des solutions de type **Pi-hole** ou **AdGuard Home** avec des listes de blocage agressives ciblant les domaines de télémétrie connus (vortex.data.microsoft.com, telemetry.ea.com).

    - Bloquer au niveau du pare-feu périmétrique les plages d'IP brutes identifiées (23.101.x.x, 40.90.x.x) pour empêcher le contournement du DNS.
3. **Utilisation de Pare-feux Applicatifs (Portmaster) :** Utiliser des outils comme **Portmaster** (Safing) pour surveiller et bloquer les connexions par processus. Cela permet de bloquer l'accès internet de XboxPcApp.exe ou EABackgroundService.exe lorsqu'aucun jeu n'est lancé, tout en autorisant le trafic légitime si nécessaire.[62]
4. **Scripts de Nettoyage de Processus :** Mettre en place des scripts (PowerShell/Batch) qui tuent systématiquement les processus d'arrière-plan (taskkill /f /im EABackgroundService.exe) immédiatement après la fermeture du jeu.[64]

7.2 Recommandations Politiques et Organisationnelles

1. **Interdiction sur Postes Sensibles :** Proscrire formellement l'installation de tout client de jeu (Xbox, Steam, Epic, EA, Ubisoft) sur les postes de travail professionnels, même en télétravail (séparation physique des machines).
2. **Audit des Flux Sortants :** Intégrer la surveillance des connexions vers AWS Global Accelerator et les IP Azure dans les tableaux de bord SIEM (Security Information and Event Management) pour détecter les anomalies de volume (exfiltration massive).

---

8. Conclusion

L'analyse des logs réseaux et des mécanismes internes des clients Xbox, EA et Ubisoft confirme l'existence d'une **Exfiltration Silencieuse**. Ces applications ne sont pas neutres ; elles sont les capteurs terminaux d'un vaste réseau de surveillance.

1. **Vecteur Technique :** Les « File System Watchers » et les services persistants transforment les PC en sondes d'indexation, exfiltrant les données via des tunnels chiffrés et obfusqués vers AWS et Azure.
2. **Motivation Économique :** Ces données alimentent le système prédictif Aladdin de BlackRock, permettant une modélisation comportementale du marché sans précédent, dans une logique de capitalisme de surveillance.
3. **Vulnérabilité Géopolitique :** L'hégémonie du cloud américain soumet ces données au CLOUD Act et à FISA 702, offrant aux services de renseignement US un accès illimité à la vie numérique mondiale.

Pour toute entité soucieuse de la confidentialité de ses données et de sa souveraineté, la présence de ces logiciels sur un réseau non isolé constitue un risque inacceptable. L'ère de l'innocence vidéoludique est révolue ; le jeu vidéo est devenu un front actif de la guerre de l'information.

Rapport compilé par : Analyste Senior, Cyber-Espionage & Audit d'Infrastructure Critique.

Date : 10 Février 2026.

Ouvrages cités

1. Security risk: EA Background Service runs as root on Mac | EA Forums - 7498418, dernier accès : février 10, 2026, https://forums.ea.com/discussions/ea-app-technical-issues-en/security-risk-ea-background-service-runs-as-root-on-mac/7498418
2. Re: EA ap Background Service keeps running while EA app is stopped - EA Forums, dernier accès : février 10, 2026, https://forums.ea.com/discussions/ea-app-technical-issues-en/re-ea-ap-background-service-keeps-running-while-ea-app-is-stopped/7623126
3. XboxPcApp.exe Windows process - What is it? - File.net, dernier accès : février 10, 2026, https://www.file.net/process/xboxpcapp.exe.html
4. Can not launch the xbox app anymore after update : r/XboxSupport - Reddit, dernier accès : février 10, 2026, https://www.reddit.com/r/XboxSupport/comments/1gteffb/can_not_launch_the_xbox_app_anymore_after_update/
5. Xbox app keeps crashing : r/XboxGamePass - Reddit, dernier accès : février 10, 2026, https://www.reddit.com/r/XboxGamePass/comments/ic742b/xbox_app_keeps_crashing/
6. Filesystem — list of Rust libraries/crates // Lib.rs, dernier accès : février 10, 2026, https://lib.rs/filesystem
7. FileSystemWatcher used to watch for folder/file open - Stack Overflow, dernier accès : février 10, 2026, https://stackoverflow.com/questions/14779616/filesystemwatcher-used-to-watch-for-folder-file-open
8. [HELP] EC2 CPU is being maxed out by Windows Antimalware : r/aws - Reddit, dernier accès : février 10, 2026, https://www.reddit.com/r/aws/comments/11qn743/help_ec2_cpu_is_being_maxed_out_by_windows/
9. 0000486: a new STACKTRC.TXT - Bug Tracking System for SSP, dernier accès : février 10, 2026, https://bts.shillest.net/view.php?id=486
10. Optional diagnostic data for Windows 11 and Windows 10 - Microsoft Learn, dernier accès : février 10, 2026, https://learn.microsoft.com/en-us/windows/privacy/optional-diagnostic-data
11. Analysis of how exactly Windows 10 spies on you : r/linuxmasterrace - Reddit, dernier accès : février 10, 2026, https://www.reddit.com/r/linuxmasterrace/comments/3gq4uq/analysis_of_how_exactly_windows_10_spies_on_you/
12. Configure Windows diagnostic data in your organization - Windows Privacy | Microsoft Learn, dernier accès : février 10, 2026, https://learn.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization

13. Privacy Implications of Windows 10 Telemetry: Summary: Top Domains for Windows 10 Telemetry Over HTTPS, dernier accès : février 10, 2026, https://www.pcministry.com/win10_telemetry/summary/top_domains_for_telemetry_over_https/
14. Background service uses insane amount of wifi data | EA Forums - 7502746, dernier accès : février 10, 2026, https://forums.ea.com/discussions/ea-app-technical-issues-en/background-service-uses-insane-amount-of-wifi-data/7502746
15. EABackgroundService.exe running without any EA programs running. : r/origin - Reddit, dernier accès : février 10, 2026, https://www.reddit.com/r/origin/comments/oe7kzl/eabackgroundserviceexe_running_without_any_ea/
16. Re: EA ap Background Service keeps running while EA app is stopped - EA Forums, dernier accès : février 10, 2026, https://forums.ea.com/discussions/ea-app-technical-issues-en/re-ea-ap-background-service-keeps-running-while-ea-app-is-stopped/7623127
17. Re: EA Background Service opens up every time the PC is on. | EA Forums - 7549678, dernier accès : février 10, 2026, https://forums.ea.com/discussions/ea-app-technical-issues-en/re-ea-background-service-opens-up-every-time-the-pc-is-on-/7549678
18. EA ap Background Service keeps running while EA app is stopped | EA Forums - 7623113, dernier accès : février 10, 2026, https://forums.ea.com/discussions/ea-app-technical-issues-en/ea-ap-background-service-keeps-running-while-ea-app-is-stopped/7623113
19. EABackgroundService.exe Windows process - What is it? - File.net, dernier accès : février 10, 2026, https://www.file.net/process/eabackgroundservice.exe.html
20. Performance better in browser than XBox windows 10 app (and other observations) - Reddit, dernier accès : février 10, 2026, https://www.reddit.com/r/xcloud/comments/zxqdg9/performance_better_in_browser_than_xbox_windows/
21. Xcloud runs better in Google Chrome than native apps on windows and on android - Reddit, dernier accès : février 10, 2026, https://www.reddit.com/r/xcloud/comments/p77nlz/xcloud_runs_better_in_google_chrome_than_native/
22. Identifying suspicious encrypted traffic [duplicate] - Information Security Stack Exchange, dernier accès : février 10, 2026, https://security.stackexchange.com/questions/63651/identifying-suspicious-encrypted-traffic
23. 1e100.net consuming a large amount of data recently in Google Chrome. - Reddit, dernier accès : février 10, 2026, https://www.reddit.com/r/chrome/comments/6tdyeb/1e100net_consuming_a_large_amount_of_data/
24. What is 1e100.net and why do I have TCP ports open to it? - Super User, dernier accès : février 10, 2026, https://superuser.com/questions/75841/what-is-1e100-net-and-why-do-i-have-tc

p-ports-open-to-it
25. Preventing software conflicts with Ubisoft games | Ubisoft Help, dernier accès : février 10, 2026, https://www.ubisoft.com/en-us/help/connectivity-and-performance/article/preventing-software-conflicts-with-ubisoft-games/000061015
26. UPC.EXE Entry Point KERNEL32.dll - Windows 7 Ubisoft Connect :: Steam Discussions, dernier accès : février 10, 2026, https://steamcommunity.com/discussions/forum/0/3971673333118124096/
27. Understanding AWS Global Accelerator use cases, dernier accès : février 10, 2026, https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html
28. AWS Global Accelerator - network acceleration service, dernier accès : février 10, 2026, https://aws.amazon.com/global-accelerator/
29. amazon web services - EC2: Huge spike in incoming network traffic - Stack Overflow, dernier accès : février 10, 2026, https://stackoverflow.com/questions/59289370/ec2-huge-spike-in-incoming-network-traffic
30. Global accelerator is ruining my ping in the game. : r/aws - Reddit, dernier accès : février 10, 2026, https://www.reddit.com/r/aws/comments/lhwu5b/global_accelerator_is_ruining_my_ping_in_the_game/
31. Pricing for AWS Global Accelerator, dernier accès : février 10, 2026, https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-pricing.html
32. AWS Global Accelerator Pricing - Amazon Web Services, dernier accès : février 10, 2026, https://aws.amazon.com/global-accelerator/pricing/
33. Windows update using insecure and random IPs - Microsoft Q&A, dernier accès : février 10, 2026, https://learn.microsoft.com/en-us/answers/questions/5669140/windows-update-using-insecure-and-random-ips
34. Network requirements - Microsoft Defender for Cloud Apps, dernier accès : février 10, 2026, https://learn.microsoft.com/en-us/defender-cloud-apps/network-requirements
35. Azure IP Ranges and Service Tags – Public Cloud - Microsoft, dernier accès : février 10, 2026, https://www.microsoft.com/en-us/download/details.aspx?id=56519
36. Windows 10 Sends Your Data 5500 Times Every Day Even After Tweaking Privacy Settings, dernier accès : février 10, 2026, https://www.reddit.com/r/privacy/comments/98maf8/windows_10_sends_your_data_5500_times_every_day/
37. Five tips for dealing with Windows 10 telemetry - 4sysops, dernier accès : février 10, 2026, https://4sysops.com/archives/five-tips-for-dealing-with-windows-10-telemetry/
38. In our tests, some of the Microsoft hosts detected in the Windows 10 HOSTS fil... |

Hacker News, dernier accès : février 10, 2026, https://news.ycombinator.com/item?id=24050344
39. Tracking Vanguard/Blackrock Corporate Ownership, dernier accès : février 10, 2026, https://blackrockvanguardwatch.com/
40. Who Owns Microsoft? Top Shareholders Exposed (2026), dernier accès : février 10, 2026, https://hypestkey.com/who-owns-microsoft/
41. Who owns Electronic Arts? - Electronic Arts Stock Ownership - Bullfincher, dernier accès : février 10, 2026, https://bullfincher.io/companies/electronic-arts/ownership
42. EA Electronic Arts Inc Stock Ownership - Who owns Electronic Arts? - WallStreetZen, dernier accès : février 10, 2026, https://www.wallstreetzen.com/stocks/us/nasdaq/ea/ownership
43. Aladdin partners with AWS as multi-cloud adoption accelerates - Preqin, dernier accès : février 10, 2026, https://www.preqin.com/news/aladdin-partners-with-aws-as-multi-cloud-adoption-accelerates
44. BlackRock's Aladdin platform achieves cutting edge of high performance with Azure Ultra Disk Storage | Microsoft Customer Stories, dernier accès : février 10, 2026, https://www.microsoft.com/en/customers/story/25275-blackrock-financial-management-azure-ultra-disk-storage
45. Aladdin on AWS delivers cloud choice and flexibility - BlackRock, dernier accès : février 10, 2026, https://www.blackrock.com/aladdin/discover/press-release-blackrock-partners-with-aws-to-deliver-aladdin-cloud-infrastructure
46. Generative AI in Banking Financial Services and Insurance A Guide To Use Cases - Scribd, dernier accès : février 10, 2026, https://ru.scribd.com/document/807783877/Generative-AI-in-Banking-Financial-Services-and-Insurance-a-Guide-to-Use-Cases
47. Stock Market Disruption Predictions and Industry Analysis 2025 — Bold Forecasts Through 2035 (Published November 14, 2025) - Sparkco AI, dernier accès : février 10, 2026, https://sparkco.ai/blog/stock-market
48. The Hidden Equation Of Cyber Risk: Humans, Machines And Money - Forbes, dernier accès : février 10, 2026, https://www.forbes.com/councils/forbestechcouncil/2025/11/14/the-hidden-equation-of-cyber-risk-humans-machines-and-money/
49. Why Fintech Startups Need Smart Analytics - Entrepreneur, dernier accès : février 10, 2026, https://www.entrepreneur.com/science-technology/why-fintech-startups-need-smart-analytics/295681
50. Surveillance capitalism - Wikipedia, dernier accès : février 10, 2026, https://en.wikipedia.org/wiki/Surveillance_capitalism
51. Clarifying Lawful Overseas Use of Data (CLOUD) Act - Amazon Web Services, dernier accès : février 10, 2026, https://aws.amazon.com/compliance/cloud-act/
52. CLOUD Act and FISA 702: Is your cloud data truly sovereign? - Civo.com, dernier

accès : février 10, 2026, https://www.civo.com/blog/is-your-cloud-truly-sovereign
53. U.S. Laws Reshape Digital Sovereignty for IAM - Thales, dernier accès : février 10, 2026, https://cpl.thalesgroup.com/blog/access-management/digital-sovereignty-iam-us-laws
54. FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act, dernier accès : février 10, 2026, https://www.congress.gov/crs-product/R48592
55. State Platform Capitalism - Cambridge University Press, dernier accès : février 10, 2026, https://www.cambridge.org/core/elements/state-platform-capitalism/82C6895073E507A9D21D33838983767E
56. EU Privacy Law and U.S. Surveillance - CIRSD, dernier accès : février 10, 2026, https://www.cirsd.org/en/horizons/horizons-winter-issue-20/eu-privacy-law-and-us-surveillance
57. Expert opinion on US surveillance laws highlights FISA risk for data transfers to the US, dernier accès : février 10, 2026, https://www.dlapiper.com/en-us/insights/publications/2022/02/expert-opinion-on-us-surveillance-laws-highlights-fisa-risk-for-data-transfers-to-the-us
58. Jumpshot Settlement - FAQs - Avast Support, dernier accès : février 10, 2026, https://support.avast.com/en-gb/article/jumpshot-settlement-faqs/
59. FTC Order Will Ban Avast from Selling Browsing Data for Advertising Purposes, Require It to Pay $16.5 Million Over Charges the Firm Sold Browsing Data After Claiming Its Products Would Block Online Tracking | Federal Trade Commission, dernier accès : février 10, 2026, https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-ban-avast-selling-browsing-data-advertising-purposes-require-it-pay-165-million-over
60. Leaked Documents Expose the Secretive Market for Your Web Browsing Data - VICE, dernier accès : février 10, 2026, https://www.vice.com/en/article/avast-antivirus-sells-user-browsing-data-investigation/
61. FTC hits Avast with $16.5 million fine over allegations of selling users' browsing data, dernier accès : février 10, 2026, https://therecord.media/avast-fine-ftc-alleged-browser-data-sales
62. Settings Handbook - Safing Docs, dernier accès : février 10, 2026, https://docs.safing.io/portmaster/settings
63. Portmaster: The ULTIMATE Firewall and Network Manager - YouTube, dernier accès : février 10, 2026, https://www.youtube.com/watch?v=8p0XIG_RYQg
64. XboxDevModeBatchScripts/removetelemetry.bat at main - GitHub, dernier accès : février 10, 2026, https://github.com/xboxoneresearch/XboxDevModeBatchScripts/blob/main/removetelemetry.bat
65. Anyone else's EA app is ALWAYS BROKEN?? : r/LowSodiumSimmers - Reddit, dernier accès : février 10, 2026, https://www.reddit.com/r/LowSodiumSimmers/comments/1di3phs/anyone_elses_

ea_app_is_always_broken/