BTS SIO

Dossier de Veille

Roca Delphin

2025 – 2028

Sommaire

Introduction — Pourquoi le cloud seul ne suffit plus face aux contraintes de l'IoT

L'Internet des objets (IoT) regroupe des **équipements connectés** (capteurs, routeurs, caméras, objets domotiques ou industriels) capables de **collecter** et **transmettre** des données. Avec leur multiplication, les systèmes IoT produisent des flux continus et doivent parfois réagir en temps réel (alertes, automatisations, sécurité).
Beaucoup d'architectures IoT reposent sur le cloud computing, qui centralise le stockage et le traitement sur des serveurs distants accessibles via Internet. Or, le modèle "tout cloud" atteint vite ses limites : latence, bande passante, dépendance au réseau et gestion de données sensibles.

Parallèlement, l'IoT est devenu une cible majeure : des appareils mal sécurisés peuvent être détournés en botnets IoT pour lancer des attaques DDoS ou servir d'infrastructure malveillante. Ces attaques mettent sous pression les services exposés sur Internet et montrent que la sécurité doit aussi se jouer au plus près des objets.

Dans ce contexte, le Edge Computing consiste à traiter une partie des données près des objets connectés (sur l'objet, une passerelle ou un serveur local) afin d'améliorer la réactivité et de limiter les contraintes du cloud.

Problématique

En quoi le Edge Computing répond-il aux limites du Cloud Computing dans les systèmes IoT ?

Plan du dossier

- **I.** Botnets IoT et attaques DDoS : comprendre la menace et la fragilité des objets connectés
- **II.** Quatre cas concrets récents pour illustrer les méthodes et impacts
- **III.** Edge Computing : répondre aux limites du "tout cloud" (latence, bande passante, résilience, confidentialité, sécurité)
- **IV.** Sécuriser un système IoT avec une approche edge : mesures essentielles à mettre en place

Méthodologie de veille

Sélection de sources techniques et institutionnelles, croisées avec de la presse spécialisée, afin de vérifier les informations et relier chaque cas étudié à la problématique.

I. Quand l'IoT devient une arme : comprendre la montée des botnets et des attaques DDoS

1) Botnets IoT : comment des objets connectés sont détournés

Un **botnet IoT** est un réseau d'objets connectés compromis (routeurs, caméras IP, box, DVR…) contrôlés à distance par un attaquant. Une fois infecté, l'appareil devient un **"bot"** : il exécute des ordres (scanner Internet, se propager, envoyer du trafic malveillant).
Ce phénomène est particulièrement fréquent dans l'IoT car de nombreux équipements restent en service longtemps, avec des **mises à jour irrégulières**, des **mots de passe faibles** ou des **services exposés**. Les attaquants ciblent souvent les équipements situés "en bordure" du réseau (routeurs domestiques/PME), car ils sont très nombreux et rarement sécurisés comme un parc informatique professionnel.

2) Attaques DDoS : des records qui mettent sous pression les services cloud

Une attaque **DDoS** (*déni de service distribué*) consiste à saturer une cible (site web, API, service en ligne) par un volume énorme de requêtes ou de paquets réseau. L'IoT est un "carburant" idéal pour ces attaques : un grand nombre de petits appareils, coordonnés, peut générer une puissance massive.
Ces attaques posent un problème direct au modèle **"tout cloud"** : si toute l'infrastructure dépend d'un point d'entrée central (services cloud, API publiques), alors un pic de trafic peut provoquer une **indisponibilité**, une **dégradation de performance** et parfois des **coûts importants** (bande passante, mitigation, surdimensionnement).
En clair : plus l'IoT se développe, plus le cloud doit absorber des flux extrêmes — ce qui renforce l'intérêt de traiter et filtrer une partie du trafic **au plus près des objets** (edge).

3) Pourquoi l'IoT est fragile : fin de support, failles réutilisées, effet "shotgun"

Les botnets actuels ne reposent pas seulement sur des mots de passe faibles : ils exploitent aussi des **vulnérabilités connues** sur des appareils **non mis à jour**, parfois parce qu'ils sont en **fin de support (EoL)**. Quand un équipement n'est plus maintenu, il devient une cible facile et durable.
Autre tendance : l'approche dite **"shotgun"** (tir en rafale). Le botnet tente automatiquement plusieurs failles sur une grande diversité d'appareils (routeurs, caméras, enregistreurs…). Dès qu'un appareil répond à une vulnérabilité, il est compromis, puis ajouté au botnet.
Résultat : la constitution du botnet est plus rapide, plus large, et l'attaque peut toucher des milliers d'équipements dispersés dans le monde.

II. Quatre cas concrets qui illustrent la menace actuelle

1) AISURU — La puissance brute des botnets IoT au service du DDoS

Le botnet **Aisuru** illustre une réalité simple : des objets connectés compromis peuvent produire des attaques DDoS d'une intensité hors norme. Dans son rapport **T3 2025**, Cloudflare explique avoir atténué **1 304 attaques hyper-volumétriques** attribuées à Aisuru sur le seul trimestre (+54% vs T2), dont une attaque record annoncée à **29,7 Tbps** et une autre à **14,1 Bpps**.
Ces pics extrêmes, parfois très courts, suffisent à mettre en défaut des services exposés (API, plateformes, portails) si la défense n'est pas dimensionnée et automatisée.

À retenir

- Un botnet IoT peut générer des attaques **massives** avec une armée d'appareils disséminés.
- Les records (Tbps / Bpps) mettent surtout en évidence la pression sur les **points d'entrée centralisés** (souvent côté cloud).
- **Lien problématique :** plus l'architecture dépend d'un accès central, plus elle devient sensible aux pics → intérêt de **filtrer / limiter / répartir** au plus près du réseau (logique edge).

2) Operation WrtHug — Quand des routeurs deviennent une infrastructure invisible

Ici, l'objectif n'est pas de "faire tomber" un service, mais de fabriquer une **infrastructure discrète** à partir d'équipements domestiques/PME. La campagne **WrtHug** décrit la compromission de **plus de 50 000 routeurs ASUS**, en exploitant des vulnérabilités connues sur le service **AiCloud** (accès à des fichiers locaux via Internet).
Les analyses associent cette opération à une logique d'**Operational Relay Box (ORB)** : utiliser des routeurs compromis comme relais/proxy pour masquer d'autres activités (commandement, espionnage, rebonds).

À retenir

- Le routeur (edge naturel) est une cible idéale : présent partout, rarement surveillé.
- Les appareils **EoL** (fin de support) restent exposés longtemps, donc rentables pour les attaquants.

- **Lien problématique :** déplacer du traitement vers l'edge n'a de sens que si l'edge est **durci** (MAJ, services exposés réduits), sinon il devient un **point d'entrée**.

3) RondoDox — "Exploit shotgun" : contaminer en tirant sur tout ce qui dépasse

RondoDox représente l'industrialisation du compromis : au lieu de dépendre d'une seule faille, le botnet tente **des dizaines de vulnérabilités** sur **de nombreux modèles** jusqu'à obtenir une prise. BleepingComputer et Trend Micro décrivent une campagne active depuis **juin 2025**, visant **56 vulnérabilités** sur **plus de 30 types d'équipements** (DVR/NVR, CCTV, routeurs, serveurs web exposés, etc.).
Le mécanisme est simple : il suffit qu'un parc ait quelques équipements oubliés, exposés et non patchés, pour alimenter la croissance du botnet.

À retenir

- Le "shotgun" marche parce que l'IoT est hétérogène et souvent mal maintenu.
- Beaucoup de failles ciblées sont des **n-day** : elles sont connues et parfois corrigées, mais les appareils restent non mis à jour.
- **Lien problématique :** l'edge peut aider (filtrage, blocage, détection locale), mais il ne compense pas l'absence de **patch management**.

BadBox 2.0 — Des appareils du quotidien transformés en fraude et en proxy

BadBox 2.0 montre que l'IoT "dangereux" n'est pas seulement industriel : ce sont aussi des appareils grand public. Google explique que le botnet a compromis **plus de 10 millions d'appareils non certifiés** utilisant **Android Open Source Project (AOSP)**, avec du malware souvent **préinstallé**, puis exploité pour de la **fraude publicitaire** et d'autres usages criminels.
Le FBI a également alerté sur l'usage de BadBox 2.0 pour faciliter des activités criminelles via des équipements connectés domestiques (boîtiers TV, projecteurs, cadres numériques, etc.).

À retenir

- Quand l'infection est **en amont** (préinstallée), le "cloud" ne protège pas l'utilisateur à lui seul.
- Les appareils compromis peuvent servir de **proxy**, ce qui rend l'attribution et le blocage plus complexes.
- **Lien problématique :** une approche edge (segmentatio

III. Edge Computing : rapprocher le traitement pour dépasser les limites du « tout cloud » en IoT

Dans un système IoT “tout cloud”, les objets envoient leurs données vers des serveurs distants qui stockent, analysent et déclenchent des réponses. Ce modèle centralise bien la supervision, mais il devient vite contraignant dès qu’il faut réagir vite, gérer beaucoup de données ou faire face à une connexion instable. Le **Edge Computing** déplace une partie du traitement près des objets (objet, passerelle, serveur local) pour réduire la distance et mieux contrôler les flux.

Limites du “tout cloud” en IoT

- **Latence** : aller-retour vers le cloud trop lent pour certains usages.
- **Bande passante** : flux bruts trop lourds à transporter en continu.
- **Dépendance réseau** : coupure = service fortement dégradé.
- **Données sensibles** : tout remonter n’est pas toujours nécessaire.

Apports concrets de l’edge

- **Décision locale** : action immédiate sans attendre le cloud.
- **Filtrage/agrégation** : le cloud reçoit l’essentiel (événements, indicateurs).
- **Résilience** : continuité en mode dégradé + synchronisation ensuite.

Sécurité (point clé)

- **Détection plus tôt**, **flux sortants limités**, **isolement rapide** d’un équipement suspect.
  !! À condition d’assurer mises à jour, durcissement et supervision des passerelles/serveurs edge. !!

Schéma

Objets IoT → Edge (filtre + décision + continuité + contrôle local) → Cloud (historique + supervision + analyse globale)

IV. Sécuriser un système IoT avec une approche Edge : ce qu'il faut mettre en place

IV. Sécuriser un système IoT avec une approche Edge : ce qu'il faut mettre en place

Une architecture **Edge + Cloud** n'est utile en sécurité que si l'edge est géré comme un élément critique. L'objectif est de contrôler ce qui se passe à la périphérie, là où l'IoT est le plus souvent attaqué.

D'abord, il faut **reprendre la main sur les équipements** : connaître précisément les objets et passerelles en service, maintenir les firmwares, retirer les matériels **fin de support** et supprimer les identifiants par défaut. Sans cette base, l'IoT reste un ensemble d'appareils faciles à détourner.

Ensuite, on réduit les **portes d'entrée**. Beaucoup de compromissions démarrent par des services exposés inutilement : l'administration doit être limitée à un réseau interne, et l'accès à distance encadré plutôt que laissé ouvert sur Internet.

Le point le plus décisif dans une approche edge reste le **contrôle des communications** : segmentation du réseau IoT et filtrage sortant. Même si un appareil est compromis, ces règles empêchent qu'il rejoigne un botnet, scanne le réseau ou serve de relais.

Enfin, l'edge doit permettre une **réaction locale** : repérer un comportement anormal et isoler rapidement un équipement (quarantaine), puis corriger avant de le remettre en service. Cette capacité de containment sur place limite l'impact et évite la propagation.

Conclusion

Ce dossier de veille montre que les menaces IoT actuelles (botnets, DDoS, exploitation en chaîne de failles) exploitent souvent la périphérie du réseau : routeurs, caméras, boîtiers et équipements peu maintenus. Dans ce contexte, le modèle "tout cloud" atteint ses limites, car il dépend d'un accès centralisé, subit la latence, la bande passante et reste vulnérable aux coupures réseau. Le **Edge Computing** apporte une réponse concrète en rapprochant le traitement : décisions plus rapides, flux mieux maîtrisés, continuité locale et contrôle de proximité. Sur le plan cyber, l'edge permet surtout de détecter plus tôt, limiter les communications sortantes et isoler un équipement suspect avant qu'il ne participe à un botnet ou à une attaque DDoS. Toutefois, ces bénéfices n'existent que si l'edge est administré sérieusement (mises à jour, durcissement, segmentation, supervision). Au final, l'approche la plus solide reste **hybride Edge + Cloud** : l'edge pour le temps réel et la sécurité terrain, le cloud pour l'historique, la supervision globale et l'analyse à grande échelle.

Sources

https://blog.cloudflare.com/ddos-threat-report-2025-q3/
https://www.cloudflare.com/de-de/threat-intelligence/research/report/aisuru-botnet/

https://securityscorecard.com/blog/operation-wrthug-the-global-espionage-campaign-hiding-in-your-home-router/
https://www.securityweek.com/over-50000-asus-routers-hacked-in-operation-wrthug/

https://www.f5.com/labs/articles/tracking-rondodox-malware-exploiting-many-iot-vulnerabilities
https://www.bleepingcomputer.com/news/security/rondodox-botnet-targets-56-n-day-flaws-in-worldwide-attacks/
https://www.theregister.com/2025/10/09/rondodox_botnet_fires_exploit_shotgun/

https://blog.google/technology/safety-security/google-taking-the-hackers-to-court-over-the-badbox-20-botnet/

https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://nvd.nist.gov/vuln/detail/CVE-2018-4063

https://www.etsi.org/technologies/multi-access-edge-computing
https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-edge/10/
https://www.enisa.europa.eu/news/unveiling-the-telecom-cybersecurity-challenges-of-esims-of-fog-and-edge-computing-in-5g
https://www.nist.gov/publications/analyzing-data-privacy-edge-systems