Cette bibliothèque Rust téléchargée plus de 50 millions de fois cachait un malware

Par Mélina Loupia

Publié le 21 août 2026 à 07h09

Des pirates viennent de publier sur crates.io, une version piégée de la bibliothèque Rust arrayref, téléchargée 53 millions de fois au cours des quatre-vingt-dix derniers jours. Le code malveillant volait les identifiants enregistrés dans Chrome, Brave et Edge. Crates.io a retiré le paquet moins d'une heure après sa publication.

Cette bibliothèque Rust téléchargée plus de 50 millions de fois cachait un malware - ©Lloyd Carr / Daniel Drew

Rust sert à écrire des composants critiques, des systèmes d'exploitation aux navigateurs, en limitant les risques de corruption mémoire. Arrayref sert à manipuler des tableaux dans ce langage sans copie de données, une opération [illegible] ents Rust sur quatre l'utilisent. La bibliothèque [illegible] éation, selon *Wiz*. La

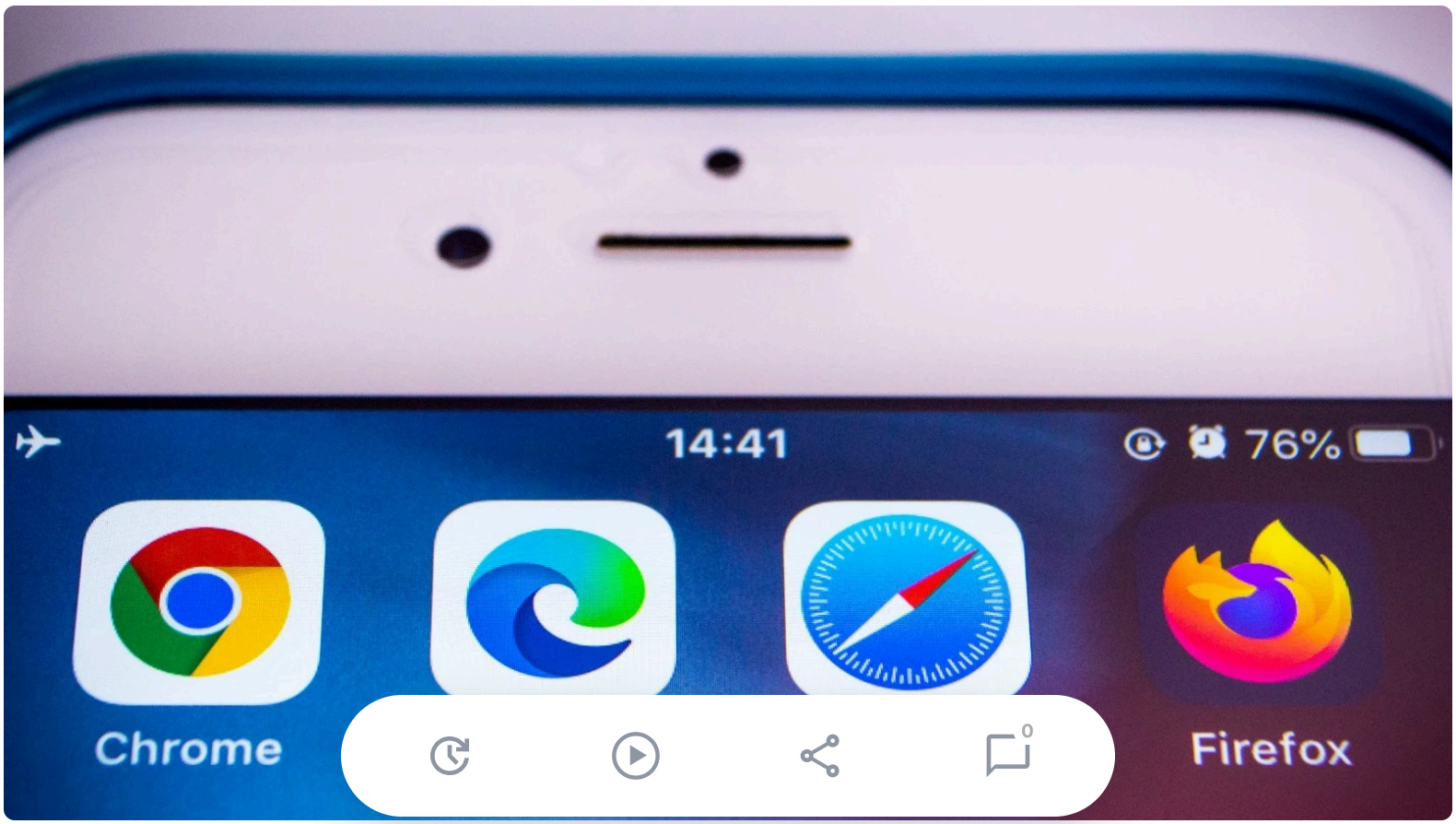
version 0.3.10, publiée le 20 août, embarquait une dépendance, proc-macro1, calquée sur le nom du paquet légitime proc-macro2. Le compilateur déclenchait le fichier build.rs de cette dépendance dès la compilation, avant toute exécution du projet. Le script reconstituait ensuite un programme à partir de fragments encodés en base64, puis récupérait une charge adaptée au système d'exploitation de la machine visée.

Il suffisait de compiler un projet dépendant de cette version pour déclencher l'infection, sans action supplémentaire du développeur. Deux autres paquets, append-only-vec et internment, comportaient cette dépendance piégée.

Un compte usurpé publie la version piégée

Les attaquants ont usurpé l'identité d'un contributeur reconnu de l'écosystème Rust pour créer un compte GitHub, à 1h17 UTC le 20 août. Depuis ce compte, ils ont publié la version 0.3.10 d'arrayref à 7h15. Trente-neuf minutes plus tard, StepSecurity, une entreprise spécialisée en sécurité des chaînes d'approvisionnement logicielles, a signalé l'incident. Le registre crates.io a réagi en supprimant la version compromise à 8h03, avant de retirer l'ensemble du paquet de son index à 8h41. Un peu plus d'une heure s'est écoulée entre la publication de la version piégée et son retrait complet de l''index.

Le compte du mainteneur historique, droundy, a été verrouillé par précaution. La charge finale du programme malveillant proposait quatre commandes, kill, minicfg, startup et runscript, et recourait à un algorithme de génération de domaines si ses serveurs de contrôle devenaient injoignables. Le programme interrogeait aussi les bases SQLite de Chrome, Brave et Edge, sur Windows, macOS et Linux, pour en extraire les identifiants enregistrés.



Le programme interrogeait aussi les bases SQLite de Chrome, Brave et Edge, sur Windows, macOS et Linux, pour en extraire les identifiants enregistrés - ©Koshiro K / Shutterstock

Wiz détecte des indices d'origine nord-coréenne

Wiz est une entreprise spécialisée dans la sécurité du cloud. Elle a relevé trois points de recoupement avec des campagnes menées par des groupes nord-coréens. Le malware d'arrayref contactait un point de contrôle, /49890878. Ce point de contrôle apparaît aussi dans la campagne Mastra, une opération menée contre d'autres écosystèmes logiciels.

Une adresse IP présente dans l'infrastructure de cette nouvelle attaque, 23.254.167.216, apparaît aussi dans les infrastructures utilisées lors du piratage de la bibliothèque JavaScript Axios, installée 83 millions de fois par semaine. Les deux attaques recourent à une plage d'adresses IP commune, 23.254.164.0/23, hébergée par Hostwinds. Google avait remonté la piste d'un groupe de cybercriminels nord-coréens après le piratage d'Axios, sans confirmer s'il s'agissait de Lazarus ou d'un autre groupe connu. Amazon avait recensé, plus tôt cette année, plusieurs cyberattaques contre des paquets npm. L'entreprise en tenait un unique groupe de pirates nord-coréens pour responsable.

Selon *Wiz* toute machine sur laquelle un projet dépendant des paquets piégés a été compilé est compromise. L'entreprise conseille de vérifier les fichiers Cargo.lock, de renouveler les identifiants enregistrés dans les navigateurs concernés et de supprimer les fichiers de persistance déposés par le programme, /tmp/rust-setup sous Unix et rust-setup.ps1 dans le dossier temporaire sous Windows.

Qu'est-ce qu'une API (Application Programming Interface) et à quoi sert-elle dans un service numérique ?

Une API est une interface qui définit comment deux logiciels peuvent échanger des données et des fonctions de manière standardisée. Elle sert à connecter des services entre eux (par exemple une appli mobile et un backend), sans exposer toute l'implémentation interne. Une bonne API précise les formats de données, les méthodes disponibles, et les règles d'authentification/autorisation. Elle facilite aussi l'intégration par des tiers, la maintenance et l'évolution du service. Dans un contexte de sécurité, elle limite ce qui est accessible et trace les accès via des clés, jetons ou signatures.

À quoi correspond une architecture « client-serveur » et en quoi impacte-t-elle les performances et la confidentialité ?

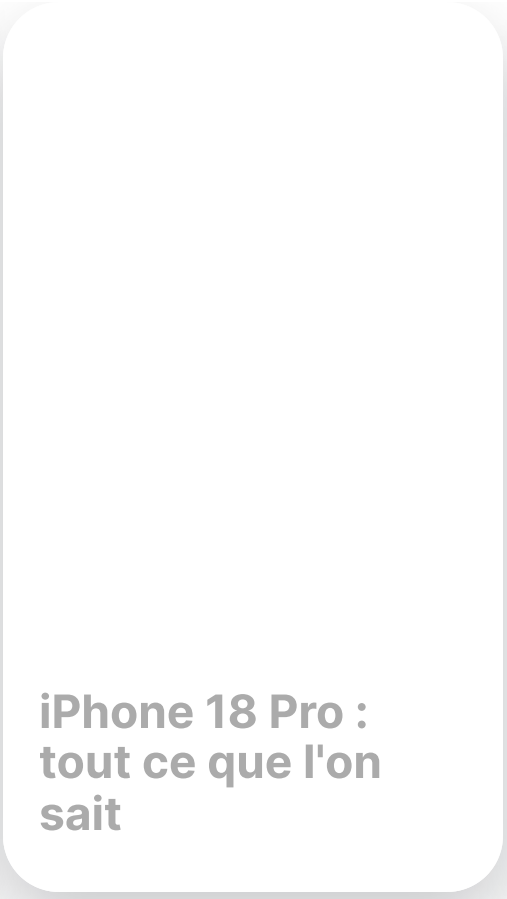
L'architecture client-serveur sépare l'interface utilisée côté appareil (le client) et les traitements/données centralisés côté serveur. Le client affiche, collecte des actions et envoie des requêtes ; le serveur répond, applique la logique métier et stocke souvent les informations. Cette séparation permet de mettre à jour rapidement les règles et fonctionnalités côté serveur, mais rend le service dépendant de la connexion réseau et de la latence. Sur la confidentialité, beaucoup dépend de ce qui est traité localement vs envoyé au serveur, et des mécanismes de chiffrement et de minimisation des données. Elle conditionne aussi la résilience : pannes, pics de charge et protections anti-abus se gèrent surtout côté serveur.

Quelle différence entre chiffrement « en transit » (TLS/HTTPS) et chiffrement « de bout en bout » (E2EE) ?

Le chiffrement en transit (TLS/HTTPS) protège les données pendant leur trajet entre un appareil et un serveur, empêchant un tiers sur le réseau de les lire. En revanche, le serveur peut généralement déchiffrer les contenus, puisqu'il termine la connexion TLS. Le chiffrement de bout en bout (E2EE) signifie que seuls les appareils des correspondants possèdent les clés permettant de lire le message : le serveur ne voit que des données chiffrées. L'E2EE renforce la confidentialité face aux fuites côté serveur, mais complique certaines fonctions (recherche serveur, modération automatique, sauvegardes lisibles). La différence tient donc surtout à qui a techniquement la capacité de déchiffrer les contenus.

Par **Mélina Loupia**

Vidéos



Vous êtes un utilisateur de **Google Actualités** ou de **WhatsApp** ?

Suivez-nous pour ne rien rater de l'actu tech !

Inscrivez-vous à notre newsletter quotidienne

Votre adresse email

Je m'inscris !

En cliquant sur s'inscrire, j'accepte de recevoir par email des informations, actualités et offres commerciales de Clubic. Conformément au RGPD, vous pouvez retirer votre consentement à tout moment en cliquant sur le lien de désinscription présent dans chaque email. Pour en savoir plus sur la gestion de vos données, consultez notre Politique de confidentialité

Commentaires 0

Participer à la discussion

Partagez votre avis avec la communauté Clubic.

Restez toujours objectif, pertinent et juste dans vos commentaires. Il est strictement interdit d'intégrer des commentaires discriminants, injurieux, racistes, sexistes, etc.
Merci de vous connecter à votre compte clubic pour laisser un commentaire.

Poster mon commentaire

Top 3 meilleurs antivirus

Bitdefender	Voir l'offre
Norton	Voir l'offre
Avast	Voir l'offre

Comparer les antivirus

- **Indépendance**
- **Transparence**
- **Expertise**

L'équipe Clubic sélectionne et teste des centaines de produits qui répondent aux usages les plus courants, avec **le meilleur rapport qualité / prix possible.**

Sur le même sujet

Amazon attribue plusieurs cyberattaques contre npm à un même groupe de hackers nord-coréens

108 malwares dévoilés : des hackers nord-coréens visaient les utilisateurs par milliers

Le c cybe accè

Abonnez-vous à notre newsletter !

Recevez un résumé quotidien de l'actu technologique.

Votre adresse e-mail

S'inscrire

En cliquant sur s'inscrire, j'accepte de recevoir par email des informations, actualités et offres commerciales de Clubic. Conformément au RGPD, vous pouvez retirer votre consentement à tout moment en cliquant sur le lien de désinscription présent dans chaque email. Pour en savoir plus sur la gestion de vos données, consultez notre **Politique de confidentialité**

Indépendance, transparence et expertise

Clubic est un média de recommandation de produits 100% indépendant. Chaque jour, nos experts testent et comparent des produits et services technologiques pour vous informer et vous aider à consommer intelligemment.

À propos

Marques tech
Événements tech
Archives
RSS

Infos légales Confidentialité CGU Modération Politique cookie Gestion des cookies