«Confusion de dépendances» : le strike à 140 000 $ d'un white hat

Apple, Microsoft, Netflix, PayPal, Tesla, Uber… La liste des entreprises qu'Alex Birsan dit avoir hackées retient l'attention. Les sommes qu'elles lui ont versées aussi : 140 000 $ au total.

Qu'a fait ce chercheur pour toucher une telle récompense ? Il a mené à bien des **attaques de type « supply chain » fondées sur ce qu'il a appelé la « confusion de dépendances »**. Son levier : du code malveillant introduit sur les dépôts tiers officiels de plusieurs langages de programmation. En l'occurrence, npm (Node.js), PyPI (Python) et RubyGems (Ruby). Son vecteur pour diffuser ce code : une vulnérabilité commune aux gestionnaires de paquets.

La réflexion avait véritablement démarré à l'été 2020. Avec un de ses pairs, Alex Birsan avait découvert, sur un dépôt GitHub public, un paquet npm apparemment destiné à un usage interne chez PayPal. Le fichier de manifeste associé faisait référence à un « mix » de dépendances : certaines présentes dans le dépôt public, d'autres hébergées en interne.

Une question s'est alors posée : s'il existait, dans le dépôt public, un paquet du même nom qu'une dépendance privée, aurait-il la priorité ? Pour y répondre, Alex Birsan a élargi son terrain de chasse.

Au 2e semestre 2020, il a collecté des centaines de noms de paquets privés, publiés accidentellement sur des dépôts publics, voire sur des forums. Essentiellement des paquets JavaScript, qui tendent, explique-t-il, à se retrouver embarqués dans des scripts publics pendant le processus de *build*.

Les paquets malveillants étaient conçus pour exécuter leur charge utile dès le *pull*. Cela ouvrait un canal d'exfiltration de données par DNS. Avec quatre éléments récupérés sur chaque machine infectée : nom d'hôte, nom d'utilisateur, dossier racine et IP externe.

Dépendances : la loi du plus haut

Constat général : sauf paramétrage spécifique, les gestionnaires **priorisent le paquet qui a le plus haut numéro de version**, peu importe où il se trouve.

Par rapport aux attaques de type *typosquatting* ou *brandjacking*, celle-ci ne suppose aucune action de la part de la victime. À moins que l'attaquant ait réussi à cloner le paquet privé, le code malveillant entraîne un plantage au moment de l'importation ou de la compilation. Mais il faut pouvoir repérer le problème, surtout avec les systèmes de *build* automatisés. En outre, l'exécution de code à distance est déjà faite quand surviennent les erreurs.

Lorsque Alex Birsan a fait le point sur ses découvertes, le compteur en était à 35 organisations touchées. Essentiellement des structures de plus de 1000 employés. Près des trois quarts des *logs* DNS reçus provenaient de paquets npm. L'un des projets affectés est vraisemblablement lié au système d'authentification Apple ID.

Microsoft a accordé la récompense maximale dans le cadre de son programme de bug bounty : 40

000 $. L'éditeur a surtout publié un guide consacré à la problématique. Il y fournit plusieurs techniques d'atténuation. Elles consistent essentiellement à restreindre le périmètre de tirage (pointage vers un dépôt privé unique, spécification de la source de chaque paquet, réservation de noms sur les dépôts tiers…) et à réaliser des vérifications d'intégrité côté client.

> *Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies*
>
> *Check the thread after reading for a few bonus facts https://t.co/00acKS0ur3*
>
> *— Alex Birsan (@alxbrsn) February 9, 2021*

Illustration principale © Dmitry Baranovskiy / CC BY 2.0