Forum: Sécurité

Topic: Cyberattaque géante

Subject: Re: Cyberattaque géante

Publié par: tignothe

Contribution le : 04/08/2021 23:18:12

Bonjour,

Citation :
Les attaques sur la chaîne … s'aggravent et nous ne sommes pas prêts

Un titre ronflant volontairement angoissant !

— « et une couche de plus » ! Le condensé de ton sentiment sur la question est d'un laconisme sidérant !

Tout d'abord l'article de ZDNet est tiré d'un rapport de l'enisa publié le 29 juillet au titre moins ronflant que je traduirais par « Panorama des menaces pour les attaques de la chaîne d'approvisionnement ». Ce qui me semble moins anxiogène.

Ce rapport dit quoi ?

Qu'une société ayant mis en place tous les moyens de défense connus reste très vulnérable par le biais de ses fournisseurs qui eux n'ont peut-être pas le même niveau de défense.

Le moyen employé la corruption de lignes de code sur un logiciel de mises à jour à permis d'ouvrir des portes sur la société cible (celle qui possède des moyens de défense sophistiqués). Car qui irait vérifier par le menu le code d'une société amie avec qui on a sous-traité des applications ou autres travaux ?

Citation :
Même la Linux Foundation se penche dessus :

— Non ! La fondation Linux donne son avis sur la manière dont les choses se sont passées.

Le code malicieux a été inséré dans l'environnement de construction du programme, donc avant la compilation du code source. Ce qui a pour conséquence de rendre caduque les consignes de sécurité habituelles à savoir ;

– N'installer que des versions logicielles signées : par la compilation le logiciel ainsi obtenu est signé.

– Mettez à jour votre logiciel ; c'est justement le moyen utilisé pour l'attaque.

– Consultez le code source : Pas sûr que dans ce cas les développeurs d'Orion aient pu repérer les changements du code source, car c'est l'environnement de construction du programme qui a été touché.

Donc parce que Orion n'est pas un logiciel open source le fait de cacher ce code n'est pas un gage de sécurité, loin s'en faut.

Finalement la Linux fondation met le doigt sur ce qui ne peut pas fonctionner. Tant que rien ne changera des sociétés de l'envergure de Microsoft resteront vulnérables.