

Transparence : Kaspersky donne accès au code source de son antivirus

A travers la « **Global Transparency Initiative** », **Kaspersky** affiche sa volonté de transparence. Et, au regard des soupçons de connivence qui pèsent sur l'éditeur de solutions de sécurité IT d'origine russe vis-à-vis des services de renseignement de son pays.

Concrètement, Kaspersky veut proposer à un tiers de confiance d'évaluer le code source de ses logiciels en vue « d'un examen indépendant ». Y compris les mises à jour et moteurs de détection des menaces.

Cette certification par un organisme tiers se fera « sous condition » (non précisée dans le communiqué). Elle a vocation à rassurer les clients, partenaires et autres parties prenantes sur l'intégrité du code.

Trois centres de transparence seront érigés sur trois plaques continentales (Europe, Asie, Etats-Unis) entre 2018 et 2020. Ce type de structure accueillera « les partenaires de confiance » et les parties prenantes des gouvernements.

Les organismes qui entrent dans le cercle de confiance au nom d'une couche supplémentaire de sécurité pourront également évaluer les processus du cycle de développement sécurisés de l'éditeur et les stratégies de gestion des risques liés aux logiciels et à la chaîne logistique.

Wanted vulnérabilité : 100 000 dollars

Qui plus est, Kaspersky pousse à 100 000 dollars la prime récompensant les chercheurs qui trouveront les vulnérabilités les plus sévères de l'anti-virus.

Une chasse aux bugs des plus motivantes pour les experts en sécurité dans le but de limiter les points faibles des solutions logicielles de l'entreprise.

En fonction des suggestions recueillies sur la vague des premières initiatives, Kaspersky peaufinera son programme de transparence. La deuxième phase débutera à partir du deuxième semestre 2018. D'ici là, l'éditeur s'engage à publier régulièrement les avancées.

Rien à cacher ?

« La balkanisation de l'Internet ne profite à personne, sauf aux cybercriminels. Une coopération réduite entre les pays favorise l'action des cybercriminels et les partenariats public-privé ne fonctionnent pas comme ils le devraient », commente Eugène Kaspersky.

« Nous devons rétablir la confiance dans les relations entre les entreprises, les gouvernements et les citoyens. C'est pourquoi nous lançons cette initiative de transparence mondiale : nous sommes totalement ouverts et nous n'avons rien à cacher. Et je crois qu'avec ces actions, nous serons capables de surmonter la méfiance et de soutenir notre engagement à protéger les personnes dans n'importe quel pays du monde. »

Les soupçons [d'accointance avec le Kremlin](#) sont entretenues en raison du passé d'Eugène Kaspersky, qui a suivi un cursus de cryptographie dans un organisme soutenu par le KGB puis a rejoint le ministère de la Défense russe en tant qu'ingénieur.

Des récentes investigations journalistiques, en particulier [celles du Washington Post](#), ont également permis de révéler des points intrigants comme la découverte par des pirates du gouvernement israélien d'outils de hacking appartenant à la NSA (services secrets américains) stockés dans le système d'information de Kaspersky Lab.

Dans la foulée, le Wall Street Journal évoquait le rôle trouble de l'éditeur moscovite [dans une affaire de vols de documents de la NSA](#).

Kaspersky bannit aux Etats-Unis

La coupe est pleine du côté des Etats-Unis. Les sénateurs décident d'exclure les solutions Kaspersky des contrats pour les marchés militaires.

De facto, c'est la sphère des administrations américaine [qui doit couper les ponts](#) avec le fournisseur de solutions de sécurité venu de l'Est.

Tandis que [le FBI recommande vivement aux entreprises américaines d'exclure les logiciels](#) de l'éditeur russe.

Parallèlement, Kaspersky réserve aussi un paquet de révélations en dévoilant les relations ténues [entre la NSA et le groupe de hackers Equation](#). On pourrait percevoir les malheurs de Kaspersky comme un retour de manivelle...

L'éditeur doit aujourd'hui redoubler ses efforts de transparence pour prouver sa bonne foi et maintenir la confiance. Et éviter que la défiance suscitée aux Etats-Unis ne fasse boule de neige sur le reste de la planète.

Sur le front de la concurrence, ces accusations s'inscrivent aussi dans un contexte de tensions avec Microsoft.

Eugène Kaspersky reprochait à la firme de Redmont une position anticoncurrentielle avec la fourniture par défaut et gratuite de Windows Defender dans Windows 10, et l'abandon, [voire la désactivation](#), des solutions de sécurité tierces.

L'affaire a donné lieu à [une plainte auprès de la Commission européenne](#) avant que le plaignant [ne se ravise](#) en regard des efforts d'adaptation consentis par Microsoft.

Lire également

[Kaspersky veut concurrencer Windows Defender avec un antivirus gratuit](#)

[Kaspersky chahuté aux US prêt à dévoiler son code source](#)

[Kaspersky ne veut plus de l'antivirus Microsoft, la Russie enquête](#)