Absolute Computrace, l'indésirable antivol de PC?

Disposer d'un logiciel antivol sur son PC peut paradoxalement générer plus de menace qu'apporter de protection. Ce sont en substance les conclusions des chercheurs de Kaspersky Lab à l'encontre d'Absolute Computrace, une solution d'Absolute Software qui permet de bloquer à distance l'accès aux données d'un PC volé, voire de le géolocaliser pour le récupérer.

Computrace se distingue notamment de nombre de ses concurrents en s'implémentant directement dans la mémoire morte (ROM) du BIOS, ce qui interdit sa désactivation logicielle (ou la rend difficile). Une opération menée par le constructeur du PC lui-même. Sauf que cette configuration faciliterait le piratage des ordinateurs concernés, estime l'éditeur de solutions de sécurité dans son rapport. *« Des individus disposant de la puissance nécessaire pour intercepter les communications sur les fibres optiques peuvent potentiellement pirater des ordinateurs sur lesquels fonctionne Absolute Computrace. Ce logiciel peut servir à implanter des spywares »*, alerte Vitaly Kamluk, chercheur principal en sécurité au sein de l'équipe internationale de chercheurs et d'analystes (GReAT) de Kaspersky Lab.

2 millions de PC concernés

Kaspersky estime à 2 millions le nombre total d'utilisateurs chez qui l'agent Computrace est activé, majoritairement aux Etats-Unis et en Russie. Mais combien ont connaissance de la présence de cet agent ? L'éditeur l'ignore. Selon le réseau Kaspersky Security Network (KSN), l'agent Computrace fonctionne de manière officielle sur les machines d'environ 150 000 utilisateurs.

Pourquoi Computrace serait-il pour autant un vecteur d'attaque et d'espionnage ? L'éditeur d'origine russe met en évidence un protocole réseau non chiffré et qui ne nécessite aucune identification du serveur distant (l'Absolute Monitoring Center en temps normal). Autant d'éléments favorables à l'exécution de code à distance, soit pour espionner les contenus et communications de la machines, soit encore pour en faire un PC zombie à des fins d'attaques en ligne ou autres campagnes de phishing et spam.

Aucune preuve d'attaque

Pour autant, Kasperky de détient aucune preuve que Computrace soit utilisé comme plate-forme d'attaques. Néanmoins, nombre d'experts s'alertent des risques potentiels. Et cela ne remonte pas d'hier. Déjà en 2009, les chercheurs de Core Labs alertaient, dans le cadre des conférences de sécurité Black Hat, des failles de sécurité que pose Computrace potentiellement. Autre problème : l'agent d'Absolute est apparu comme un malware aux yeux de certaines solutions de sécurité, nécessitant alors son classement dans les listes blanches pour éviter les alertes en faux positif.

Il n'en demeure pas moins étrange que Kaspersky se penche seulement aujourd'hui sur les faiblesses de Computrace visiblement connues depuis plusieurs années. L'éditeur justifie qu'il a

souhaité se concentrer sur les mécanismes de sécurité réseau de la solution. Un argument d'autant plus justifié qu'on est aujourd'hui toujours plus connecté.

« Un outil aussi puissant que le logiciel Absolute Computrace doit utiliser des mécanismes d'authentification et de cryptage pour continuer d'être employé à bon escient [...]. Faute de cela, ces agents orphelins continueront de passer inaperçus, offrant la possibilité d'une exploitation malveillante à distance », conclut Vitaly Kamluk qui invite Absolute à avertir les utilisateurs et leur expliquer comment désactiver l'agent litigieux.

crédit photo © Pavel Ignatov – shutterstock

Lire également

[The Mask ou Careto : la menace persistante la plus avancée à ce jour]
[Attaque DDoS en Europe : record de trafic battu]