



HEBDO

LES PIRATAGES PAR DES LOGICIELS MALVEILLANTS ONT ETE MULTIPLIES PAR SEPT DEPUIS 2020

Près de 10 millions d'appareils ont été pris pour cible par des logiciels de vol de données en 2023, ont révélé les experts de l'équipe Digital Footprint Intelligence de Kaspersky, après avoir analysé les logs d'infostealers échangés sur le Dark Web. Leurs recherches ont également permis d'établir que les cybercriminels dérobent en moyenne 50,9 identifiants de connexion par appareil infecté, ce qui signifie que les infostealers représentent une menace de plus en plus grande pour les particuliers comme pour les entreprises.

Selon la Digital Footprint Intelligence de Kaspersky, environ 10 millions d'appareils personnels et professionnels ont été compromis par des logiciels de vol de données en 2023, soit une augmentation de 643 % sur trois ans. Les données analysées sur les appareils compromis proviennent des log files malveillants activement échangés sur les Dark Web et surveillés par Kaspersky pour aider les entreprises à assurer la sécurité de leurs clients et de leurs employés.

Bien que le nombre de log files malveillants, et donc d'infiltrations enregistrées en 2023 ait connu une baisse marginale de 9 % par rapport à 2022, cela ne signifie pas que la demande des cybercriminels en matière d'identifiants et de mots de passe ait stagné pour autant. Il est possible que certaines informations d'identification compromises en 2023 soient divulguées sur le Dark Web de façon aléatoire au cours de l'année. Par conséquent, le nombre réel de piratages est probablement encore plus élevé que 10 millions. Selon les analyses opérées par les chercheurs de Kaspersky sur l'activité des log files malveillants, le nombre d'infections survenues en 2023 devrait s'élever à environ 16 millions.

Près de 51 identifiants de connexion par appareil compromis

Les cybercriminels volent en moyenne 50,9 identifiants de connexion par appareil piraté. Ils les utilisent soit pour répondre à leurs propres objectifs malveillants, notamment pour perpétrer des cyberattaques, soit pour les vendre et les distribuer librement sur le Dark Web et sur des canaux Telegram clandestins.

Parmi les informations dérobées, on retrouve entre autres des identifiants permettant d'accéder à des comptes sur les réseaux sociaux, à des services bancaires en ligne, à des portefeuilles de crypto-monnaies et à divers services d'entreprise tels que les emails ou les systèmes internes. Selon les données recueillies par Kaspersky, 443 000 sites web dans le monde ont vu leurs informations d'identification compromises au cours des cinq dernières années.

Le domaine « .com » détient le plus de comptes compromis

En ce qui concerne le nombre de comptes compromis, le domaine .com arrive en tête. Près de 326 millions d'identifiants et de mots de passe de sites web de ce domaine ont été compromis par des infostealers en 2023. Vient ensuite le domaine .br pour le Brésil, avec 29 millions de comptes compromis, puis .in, pour l'Inde, avec 8 millions, .co (Colombie) avec près de 6 millions, et .vn (Vietnam) avec plus de 5,5 millions. Dans le cas du domaine « .fr », pour la France, 4,5 millions en 2023 de comptes ont été compromis en 2023.

Source : ITCHANNEL – Avril 2024