Veille Techno : Cyberattaques – Cheval de Troie imitant Bitdefender

Des chercheurs ont révélé une campagne sophistiquée usurpant l'identité de l'antivirus Bitdefender. Les hackers ont créé un faux site très proche de l'original pour inciter les utilisateurs à télécharger un programme malveillant.

Ce téléchargement installe en réalité trois malwares :

- **VenomRAT**, cheval de Troie d'accès à distance pour contrôler et espionner l'ordinateur,
- **StormKitty**, voleur d'informations ciblant identifiants et portefeuilles crypto,
- **SilentTrinity**, outil open source pour maintenir un accès persistant via des scripts PowerShell.

Cette opération cible surtout les professionnels cherchant à renforcer leur sécurité, exploitant leur confiance envers un logiciel réputé. Elle rappelle que même des outils de sécurité peuvent être vecteurs d'infection s'ils proviennent de sources non officielles.

Cette attaque souligne la nécessité pour les organisations, en particulier celles utilisant des outils de sécurité informatique, de renforcer leurs mesures de cybersécurité, notamment en sensibilisant les collaborateurs aux risques liés à l'usurpation d'identité et aux téléchargements frauduleux, en mettant en place des systèmes avancés de détection et de filtrage des menaces, ainsi qu'en assurant une gestion rigoureuse des accès et des sources d'installation des logiciels.

Sources :

https://linformation.ma/news/high-tech/des-hackers-imitent-cet-antivirus-tres-connu-pour-diffuser-trois-malwares-voleurs-d-identifiants-et-de-cryptos/57770

https://www.msn.com/fr-fr/actualite/technologie-et-sciences/des-hackers-imitent-cet-antivirus-tr%C3%A8s-connu-pour-diffuser-trois-malwares-voleurs-d-identifiants-et-de-cryptos/ar-AA1FDXOW