Association de malwares, danger
Internet
PostÃ© par : JerryG
PubliÃ©e le : 31/7/2023 13:00:00

Les chercheurs Proofpoint, leader en matiÃ¨re de cybersÃ©curitÃ© et conformitÃ©, publie aujourd'hui de nouvelles recherches suite Ã lâidentification dâun logiciel malveillant, quâils ont nommÃ© Â« WikiLoader Â».

Leur analyse revient en dÃ©taille sur lâutilisation de ce logiciel sophistiquÃ©, jusquâÃ prÃ©sent associÃ© Ã des campagnes de diffusion du cheval de Troie bancaire Ursnif par lâacteur de la menace TA544.

Les principales conclusions de cette recherche sont les suivantes :

â¢ IdentifiÃ© pour la premiÃ¨re fois en dÃ©cembre 2022, WikiLoarder est utilisÃ© par lâacteur de la menace TA544, qui cible habituellement les entreprises italiennes. Proofpoint a depuis observÃ© le logiciel malveillant dans de multiples campagnes.

â¢ Il s'agit d'un logiciel de tÃ©lÃ©chargement sophistiquÃ©, dont l'objectif est d'installer une deuxiÃ¨me charge utile dans lâappareil infectÃ©.
â¢ Pour cela, il utilise une multitude de mÃ©canismes pour Ã©chapper au systÃ¨me de dÃ©tection et semble avoir Ã©tÃ© dÃ©veloppÃ© comme un logiciel malveillant destinÃ© Ã Ãªtre louÃ© Ã des cybercriminels triÃ©s sur le volet.

â¢ Les chercheurs Proofpoint lâont baptisÃ© WikiLoader car il envoie une requÃªte Ã WikipÃ©dia et vÃ©rifie que la rÃ©ponse contient la chaÃ®ne de caractÃ¨res "The Free".

Â« WikiLoader est un nouveau logiciel malveillant sophistiquÃ©, qui a rÃ©cemment fait surface dans le paysage des menaces cybercriminelles. AssociÃ© jusqu'Ã prÃ©sent Ã des campagnes Ursnif, il fait actuellement l'objet d'un dÃ©veloppement actif et ses auteurs semblent y apporter des modifications rÃ©guliÃ¨res afin de rester hors radars.

Il y a fort Ã parier que davantage de cybercriminels se mettent Ã lâutiliser, en particulier les acteurs de type IAB (Initial Access Brokers), qui mÃ¨nent rÃ©guliÃ¨rement des activitÃ©s menant Ã des ransomwares.

Les Ã©quipes de sÃ©curitÃ© en charge doivent Ãªtre conscientes de l'existence de ce logiciel et des activitÃ©s qui lui sont associÃ©es dans la livraison de la charge utile afin de prendre les mesures de protection nÃ©cessaire pour leur organisation Â», prÃ©cise Selena Larson, Senior Threat Researcher chez Proofpoint.

Plus d'info sur le site de Proofpoint :Â