Selon ESET Research, Lazarus s'attaque à une entreprise de fret en Afrique du Sud via une nouvelle porte dérobée

BRATISLAVA – le 8 avril 2021 – Les chercheurs d'ESET, 1er éditeur Européen de solutions de sécurité, ont découvert une nouvelle porte dérobée utilisée pour attaquer une entreprise de logistique d'Afrique du Sud, qu'ils ont baptisée Vyveva. Ils ont attribué le malware au groupe Lazarus en raison de similitudes avec les campagnes et les échantillons précédents liés au groupe. La porte dérobée comprend plusieurs fonctionnalités de cyberespionnage, telles que l'exfiltration de fichiers, et la collecte d'informations sur l'ordinateur ciblé et ses lecteurs. Elle communique avec son serveur de commande et de contrôle via le réseau Tor.

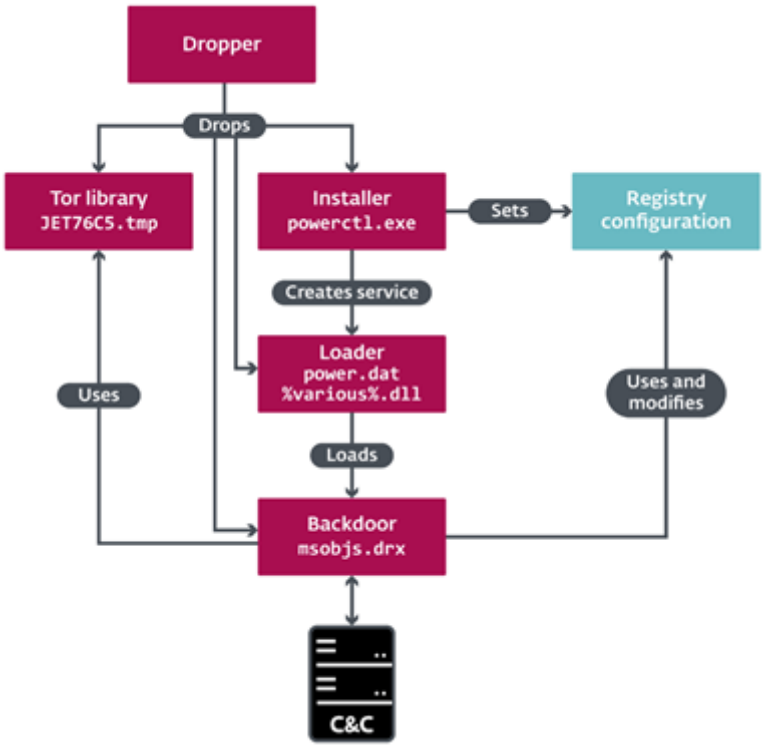
La télémétrie d'ESET pour Vyveva indique un déploiement ciblé, car les chercheurs d'ESET n'ont trouvé que deux machines victimes, toutes deux des serveurs appartenant à la société de logistique sud-africaine susmentionnée. Selon l'enquête d'ESET, Vyveva est utilisé depuis au moins décembre 2018.

« Vyveva possède de multiples similarités au niveau du code avec des échantillons plus anciens de Lazarus détectés par la technologie ESET. Ces similarités ne s'arrêtent cependant pas là : l'utilisation d'un faux protocole TLS pour la communication réseau, les chaînes des lignes de commande, les méthodes de chiffrement et l'utilisation des services Tor, pointent toutes vers Lazarus. Par conséquent, nous pouvons attribuer Vyveva à ce groupe avec quasi-certitude, » déclare Filip Jurčacko, le chercheur d'ESET qui a analysé l'arsenal découvert.

La porte dérobée exécute les commandes émises par les pirates pour effectuer des opérations sur les fichiers et les processus, et collecter des informations. Il existe également une commande moins couramment utilisée pour l'horodatage des fichiers, qui permet de copier les horodatages d'un fichier source vers un fichier destination, ou d'utiliser une date aléatoire.

Vyveva utilise la bibliothèque Tor pour communiquer avec un serveur de commande et de contrôle. Le malware contacte le serveur à intervalles de trois minutes, envoyant des informations sur l'ordinateur victime et ses lecteurs avant de recevoir des commandes. « Les fonctions de la porte dérobée utilisées pour surveiller les lecteurs nouvellement connectés et déconnectés, et pour surveiller le nombre de sessions actives, dénotant les utilisateurs connectés, présentent un intérêt particulier. Ces composants peuvent déclencher une connexion au serveur de commande et de contrôle en dehors de l'intervalle préconfiguré de trois minutes, » explique M. Jurčacko.
Pour plus de détails techniques sur Vyveva, lisez l'article « (Are you) afreight of the dark? Watch out for Vyveva, the latest addition to the Lazarus toolkit » sur WeLiveSecurity. Suivez l'actualité d'ESET Research sur Twitter.

Aperçu des composants de Vyveva



CONTACTS PRESSE

Darina SANTAMARIA : +33 01 86 27 00 39 - darina.j@eset-nod32.fr

Ines KHELIFI : +33 01 55 89 29 30 - ines.k@eset-nod32.fr

À propos d'ESET

Spécialisé dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public, ESET est aujourd'hui le 1er éditeur de l'Union européenne en matière de sécurité des endpoints. Pionnier en matière de détection proactive, ESET a été désigné pour la 2ème année consécutive, unique Challenger dans le Gartner Magic Quadrant 2019*, « Endpoint Protection » après avoir été évalué sur sa performance et sur la qualité de sa vision dans le domaine de la protection des Endpoints. À ce jour, l'antivirus ESET NOD32 détient le record mondial de récompenses décernées par le laboratoire indépendant Virus Bulletin depuis 1998. La technologie ESET protège aujourd'hui plus d'un milliard d'internautes. *Source : Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, August 20, 2019.

Pour plus d'informations : **www.eset.com/na/** Blog : www.welivesecurity.com/fr