Inès Bonvallet

Veille Technologique Passive

Black Basta - Ransomware

Les Ransomwares sont en expansion et surtout au sein des entreprises. Cette menace se développe de plus en plus et ce de différentes manières. Nous allons voir ici le Ransomware « Black Basta » qui est un des ransomware à craindre à l'heure actuelle puisqu'il a déjà attaqué plusieurs entreprises, et est géré comme un service à la demande.

Ce ransomware est considéré comme un « opérateur » de ransomware et une entreprise de Ransomware-as-a-Service (RaaS). Il est apparu en 2022 et est devenu une des menaces les plus actives du monde, accumulant 19 entreprises victimes et plus de 100 victimes confirmées. Cette attaque fonctionne par campagne de « spear-phishing » très ciblées, d'attaques par des bots mais également de chiffrement des données (désactivation de l'antivirus ou suppression de copies fantômes du système).

Mais comment surveiller et prévenir une attaque de Black Basta ?

Pour ce faire, on vérifie le nom des fichiers, par exemple qui seront aléatoires ou l'obscurcissement des chaînes (antivirus standard). Il y a aussi une extension « .basta » qui peux être ajouté aux fichiers cryptés et une note de rançon « readme.txt » sera ajoutée sur le bureau.

Enfin, pour prévenir de cette attaque, il y a plusieurs choses à faire :

- Sensibiliser les utilisateurs
- Examiner les contrôles de sécurité du réseau
- Installer et configurer des produits avancés de sécurité des points de terminaison
- Outils de gestion des identités et accès
- Stratégie de sauvegarde fiable avec des backup hors-ligne protégées

Sources :

Grâce à l'outil Feedly :

- https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/black-basta
- https://www.redpacketsecurity.com/black-basta-ransomware-victim-scrubsandbeyond-com/