Qui court le plus grand risque d'une attaque par rançongiciel, et pourquoi ces cibles sont-elles visées ?

Réponse courte : Le risque de rançongiciel dépend souvent de qui les « courtiers d'accès » criminels trouvent le plus facile à pirater, ou sont spécifiquement payés pour pirater, ce qui signifie que les écoles, les hôpitaux et les fournisseurs d'infrastructures dotés de défenses plus faibles ou de données précieuses figurent fréquemment en tête de liste.

Comment les cibles sont choisies dès le départ

Derrière la plupart des incidents de rançongiciel se cache un marché que la plupart des gens ne voient jamais. Un groupe, souvent appelé courtiers d'accès initial, passe son temps à s'introduire dans des réseaux sans plan précis quant à la suite des événements. Une fois qu'ils ont pris pied, ils mettent cet accès en vente, en décrivant exactement ce qu'ils contrôlent, comme des droits administratifs sur des outils de sécurité, la capacité de désactiver les protections antivirus, ou l'accès à une grande partie des appareils d'une organisation. Ils peuvent décrire, par exemple, avoir compromis le parc d'appareils d'un district scolaire ou les outils d'accès à distance d'un prestataire informatique. Les acheteurs, allant des groupes de vol de données aux opérateurs de rançongiciels en passant par des acteurs parrainés par des États, enchérissent alors sur cet accès en fonction de sa valeur et de son exhaustivité apparentes.

Quand les attaques sont commanditées, et non simplement opportunistes

Il existe également un second schéma, plus ciblé. Dans ce cas, un acheteur, tel qu'un groupe de rançongiciels ou un acteur étatique, formule une demande précise : trouver et compromettre un

nombre défini d'organisations répondant à certains critères, comme des hôpitaux d'une taille donnée dans une région donnée, ou des fournisseurs de services publics tels que des stations de traitement des eaux. Les courtiers d'accès traitent alors cela comme une mission commerciale, en recherchant activement des organisations correspondant au profil demandé. Une fois qu'ils réussissent, ils revendent cet accès au demandeur initial, bien que les deux parties n'interagissent généralement jamais directement et ne connaissent pas leurs identités respectives. C'est pourquoi des vagues soudaines d'attaques contre des organisations similaires, comme plusieurs hôpitaux dans une même région, reflètent souvent une commande d'achat coordonnée plutôt qu'une simple coïncidence.

Pourquoi cela compte pour la défense

Parce que le ciblage peut être à la fois opportuniste ou spécifiquement commandité, toute organisation dotée de contrôles de sécurité faibles, de données sensibles ou de services critiques peut devenir une cible, quel que soit sa taille ou son secteur d'activité. Comprendre cette dynamique acheteur-vendeur souligne pourquoi des défenses proactives et fonctionnant en permanence importent bien davantage qu'une réaction après qu'une intrusion a déjà été vendue au plus offrant.

https://player.vimeo.com/video/1047715835?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Revision #2
Created 2026-07-24 07:26:13 UTC by Dennis Underwood
Updated 2026-08-06 18:39:05 UTC by Dennis Underwood