

Que se passe-t-il réellement pendant les instants d'une attaque par ransomware ?

Réponse courte : La phase de chiffrement proprement dite d'une attaque par ransomware est remarquablement rapide, se terminant souvent en environ 60 à 90 secondes une fois déclenchée, bien que les attaquants passent un temps considérable et invisible en amont à se positionner à l'intérieur du réseau. Au moment où les symptômes visibles apparaissent, les dégâts sont déjà en train de se produire en temps réel, c'est pourquoi la détection doit intervenir avant le déclenchement final, et non après.

Le calme avant l'attaque

Avant que le ransomware ne s'active, les attaquants passent généralement du temps à se déplacer discrètement dans les systèmes de l'entreprise, à identifier les données précieuses, à désactiver les sauvegardes et à mettre en place les conditions nécessaires à une attaque réussie. Ce travail préparatoire peut passer inaperçu, car les opérations commerciales normales se poursuivent comme d'habitude. Le réseau peut sembler stable et sain jusqu'au moment où l'attaquant décide de lancer la phase finale. Un peu comme le silence inquiétant qui précède une catastrophe, cette période de calme peut être trompeuse, car elle ne reflète pas la perturbation qui est sur le point de se produire.

L'apparition rapide des dégâts

Une fois lancé, un événement de ransomware peut se dérouler en moins de deux minutes. Dans cette courte fenêtre, les employés peuvent remarquer des pannes soudaines : les e-mails cessent de fonctionner, les systèmes téléphoniques deviennent silencieux, les applications se comportent de manière erratique ou les connexions réseau deviennent instables. Ce sont des symptômes du chiffrement et de la compromission des systèmes se produisant simultanément dans l'ensemble de l'environnement. Comme le processus se déroule si rapidement, il n'y a généralement pas assez de temps pour qu'une personne intervienne manuellement une fois qu'il a commencé.

Pourquoi certains systèmes continuent de fonctionner

Un détail troublant de nombreux incidents de ransomware est que tout ne tombe pas en panne en même temps. Certains services peuvent continuer à fonctionner normalement alors que d'autres s'effondrent. Cela s'explique souvent par le fait que ces systèmes non affectés sont précisément l'endroit où l'attaquant opère encore, les utilisant comme point d'ancrage ou zone de préparation. Reconnaître ce schéma est important, car supposer qu'un problème n'est « que partiel » peut créer un faux sentiment de sécurité alors que la compromission est activement en cours. Une prévention efficace dépend de l'identification et de l'arrêt de l'activité malveillante avant que la phase destructrice finale ne commence, car une fois déclenchée, la fenêtre d'action est extrêmement courte.

<https://player.vimeo.com/video/1046658956?texttrack=fr>

[Regarder sur Vimeo](#) · Sous-titres : English, Français, Español, العربية

Revision #2

Created 2026-07-24 07:24:42 UTC by Dennis Underwood

Updated 2026-08-06 18:38:53 UTC by Dennis Underwood