Forum: Sécurité

Topic: Une Cyberattaque planétaire est en cours

Subject: Re: Une Cyberattaque planétaire est en cours

Publié par: HommeTranquille

Contribution le : 13/05/2017 17:14:19

Remarque pour les utilisateurs de Windows 10...

Certains des correctifs sont déjà actifs/opérationnels si vous êtes au dernier niveau de correctif de Windows Update ou de Defender...

Je cite (extrait) :

Aujourd'hui, beaucoup de nos clients à travers le monde et les systèmes critiques dont ils dépendent ont été victimes de logiciels malveillants "WannaCrypt". Voir les entreprises et les personnes touchées par les cyberattaques, comme ceux rapportés aujourd'hui, était pénible. Microsoft a travaillé tout au long de la journée pour nous assurer que nous avons compris l'attaque et pris toutes les mesures possibles pour protéger nos clients. Ce blog précise les étapes que chaque individu et entreprise devraient prendre pour rester protégé. En outre, nous prenons l'étape très inhabituelle consistant à fournir une mise à jour de sécurité pour tous les clients afin de protéger les plates-formes Windows qui sont uniquement en support personnalisé, y compris Windows XP, Windows 8 et Windows Server 2003. Les clients qui exécutent Windows 10 n'ont pas été ciblés par l'attaque aujourd'hui.

Les détails sont ci-dessous.

En mars, nous avons publié une mise à jour de sécurité qui traite de la vulnérabilité que ces attaques exploitent. Ceux qui ont Windows Update activé sont protégés contre les attaques de cette vulnérabilité. Pour les organisations qui n'ont pas encore appliqué la mise à jour de sécurité, nous vous suggérons de déployer immédiatement le bulletin de sécurité MS17-010 de Microsoft .

Pour les clients utilisant Windows Defender, nous avons publié une mise à jour plus tôt aujourd'hui qui détecte cette menace en tant que Ransom: Win32 / WannaCrypt . En tant que mesure "de défense en profondeur", procurez-vous un logiciel anti-malware à jour sur vos machines. Les clients qui utilisent un logiciel anti-malware de n'importe quel nombre de sociétés de sécurité peuvent confirmer auprès de leur fournisseur qu'ils sont protégés.

Ce type d'attaque peut évoluer avec le temps, de sorte que toute stratégie supplémentaire de défense en profondeur fournira des protections supplémentaires. (Par exemple, pour protéger davantage les attaques SMBv1, les clients devraient envisager de bloquer les protocoles existants sur leurs réseaux).

Nous savons également que certains de nos clients utilisent des versions de Windows qui ne reçoivent plus de support général. Cela signifie que ces clients n'auraient pas reçu la mise à jour de sécurité mentionnée ci-dessus publiée en mars. Compte tenu de l'impact potentiel pour les clients et leurs entreprises, nous avons pris la décision de mettre la mise à jour de sécurité pour les plates-formes uniquement dans le support personnalisé, Windows XP, Windows 8 et Windows Server 2003, largement disponibles pour téléchargement (voir les liens ci-dessous).

Cette décision a été prise sur la base d'une évaluation de cette situation, avec le principe de protéger l'ensemble de l'ensemble de notre écosystème client, à l'esprit.