SONICWALL

PRÉSENTATION : AU LENDEMAIN DE WANNACRY

Anatomie d'une attaque par ransomware

Résumé

Le manque d'initiative dans l'application des meilleures pratiques en matière de sécurité réseau entraîne souvent des conséquences catastrophiques. Une attaque par ransomwares d'envergure mondiale a récemment défrayé la chronique. Cette présentation se penche sur la manière dont les cybercriminels ont mené cette attaque, les défis qu'elle présente encore pour les services informatiques et les leçons à en tirer pour éviter de futures attaques.

Une histoire bien connue

C'est une histoire qui n'est que trop fréquente. Récemment, des cybercriminels ont pénétré sur le réseau d'une entreprise par le biais d'un e-mail contenant le ransomware WannaCry. La pièce jointe a été ouverte sur un ordinateur sans correctif, ce qui a eu des conséquences désastreuses. Interrogé quant à l'absence de correctif sur le système, le dirigeant de l'entreprise a répondu : « Je ne pensais pas que c'était très important. »

Anatomie d'une attaque

Il y a vraiment de quoi pleurer quand on pense à la facilité avec laquelle cette entreprise aurait pu éviter cette intrusion. Cette attaque par ransomware à grande échelle a infecté plus de 250 000 systèmes dans plus de 150 pays, dont plusieurs grands établissements de santé au Royaume-Uni et même quelques entreprises de télécommunications de premier plan en Espagne.

WannaCry n'est qu'un exemple parmi tant d'autres de menaces combinant un ransomware et un ver qui exploitent une faille du protocole de partage de fichiers SMB. On suppose qu'à l'origine, certains organismes gouvernementaux ont créé un kit d'exploit (EternalBlue en l'occurrence) que des cybercriminels auraient ensuite dérobé.

Si elles sont de plus en plus médiatisées, les attaques par ransomwares n'ont rien de nouveau. Les exploits sont quotidiens. L'excuse de l'ignorance ne dure qu'un temps.

En avril 2017, le groupe des Shadow Brokers a rendu EternalBlue accessible au public dans le cadre d'une fuite plus large d'exploits développés par la NSA. Les criminels ont ensuite utilisé les éléments de ce kit d'exploit pour développer une nouvelle forme de ransomware extrêmement agressive qui attaque, tel un ver, les machines connectées au réseau en utilisant différentes fonctions de lecture/écriture du système d'exploitation Windows. Cet exploit particulier touche différentes versions des systèmes d'exploitation Microsoft Windows, dont un certain nombre en fin de vie. Même si Microsoft a publié un grand nombre de correctifs pour résoudre cette vulnérabilité, l'attaque reste dangereuse, car beaucoup d'entreprises n'ont pas appliqué le correctif.

La première version du pack ver/ransomware avait un kill switch qui a été utilisé accidentellement pour désactiver la fonction ver, ce qui a freiné sa propagation. Cependant, les plus de 20 versions suivantes ne présentent pas ce point faible. De plus, il est important de recourir à des technologies anti-ransomwares qui bloquent toutes les versions connues et sont capables de détecter les nouvelles attaques.

Conclusion

Plus de 114 nouveaux virus et variantes sont générés toutes les soixante secondes. *WannaCry* n'est certainement pas le premier exploit à utiliser à cette forme d'attaque et ne sera sûrement pas le dernier. Les entreprises doivent prendre conscience des nouvelles réalités du champ de bataille du cyberespace mondial.

En savoir plus. Lisez notre dossier : Les 7 meilleures pratiques anti-ransomwares.

À propos de SonicWall

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

Pour toute question concernant l'usage potentiel de ce document, contactez :

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com

ExecBrief-InTheWakeOfWannaCry-US-VG-29362