Se protéger des ransomwares grâce à Zscaler™ Workload Segmentation

Sécuriser les communications est-ouest des applications et stopper le mouvement latéral des menaces

Harry Sverdlove
Directeur de la technologie, Secure Workload Communication, Zscaler

Contenu

Introduction : le système de santé américain pris en otage (une fois de plus)

En 2020, le monde est allé d'une crise à l'autre, et le monde de la cybersécurité n'a pas fait exception. Une fois de plus, l'Agence pour la cybersécurité et les infrastructures (CISA), le FBI (Federal Bureau of Investigation) et le ministère de la santé et des services sociaux (HHS) ont émis un avertissement selon lequel le secteur de la santé publique était confronté à une menace croissante liée à une campagne de ransomware. Plusieurs hôpitaux aux États-Unis avaient déjà été ciblés.

Ces attaques ne sont pas nouvelles. En 2019, l'on a enregistré plus de 140 attaques de ransomware contre les organisations gouvernementales et de santé. Au cours de la décennie écoulée, les attaques de ransomware sont devenues de plus en plus fréquentes, sophistiquées et efficaces.

Pour résumer, le ransomware est un type d'attaque dans lequel d'importants fichiers ou un système d'exploitation entier sont chiffrés à l'insu de l'utilisateur, rendant le système inexploitable jusqu'à ce que la victime (ou l'entreprise de la victime) paie une rançon (généralement en crypto-monnaie) pour obtenir la clé de déchiffrement. En d'autres termes, le ransomware est une attaque motivée par l'appât du gain et menée par des organisations cybercriminelles. En de rares occasions, ce type d'attaque est mené dans le seul but de déstabiliser l'infrastructure d'une cible, mais de manière plus générale, il est motivé par le désir de tirer profit du paiement de rançons.

Comment fonctionne le ransomware ?

Pour que les ransomwares soient efficaces, ils doivent affecter autant de systèmes que possible au sein d'un réseau. Par exemple, si sur des milliers de systèmes un seul est chiffré et désactivé, la victime est plus susceptible de déconnecter et de reconstruire ce système. Plus le nombre de systèmes ou de fichiers infestés est élevé, plus la victime sera susceptible de payer la rançon. Bien que les responsables de l'application des lois et les experts en cybersécurité recommandent *de ne jamais* payer de rançon, la réalité est que lorsqu'une entreprise perd des millions de dollars par jour en temps d'arrêt et encourt le risque de passer des semaines ou des mois à se rétablir manuellement, la tentation de résoudre le problème par un rapide paiement est compréhensible.

Dans la campagne en cours, un e-mail d'hameçonnage est envoyé aux personnes associées à une entreprise cible. Cet e-mail contient soit un logiciel malveillant (en pièce jointe), soit des liens vers un

site Web compromis qui peut inoculer la charge initiale du logiciel malveillant. Le programme malveillant initial appartient à la famille TrickBot (et ses acolytes chevaux de Troie BazarLoader/BazarBackdoor).

TrickBot est alors capable de s'installer clandestinement dans divers processus Windows, d'établir une porte discrète vers un serveur de commande et de contrôle (C&C), de télécharger des composants supplémentaires, d'utiliser des outils courants pour dresser une carte synoptique du réseau et, enfin, de se propager dans ce réseau. TrickBot possède des modules spécifiques qui peuvent se propager aux contrôleurs de domaine via un exploit SMB ou via le protocole RDP (Remote Desktop Protocol).

Au fur et à mesure que TrickBot se propage, chaque ordinateur infecté télécharge et lance le ransomware Ryuk (ou son successeur Conti), lequel est capable de chiffrer à la fois les fichiers réseau tant locaux que partagés.

Le script du ransomware est toujours le même :

1. Amener sournoisement un utilisateur à télécharger et à exécuter un fichier chargeur malveillant (ou utiliser un exploit pour le faire à son insu)
2. Faire en sorte que le fichier chargeur contacte un serveur (ou d'autres systèmes compromis) pour télécharger d'autres composants
3. Surveiller le réseau pour identifier les autres systèmes et les partages de fichiers
4. Se propager au plus grand nombre de systèmes possible, en particulier les infrastructures essentielles comme les contrôleurs de domaine
5. Chiffrer les fichiers pour désactiver entièrement le(s) système(s) ou empêcher l'accès à des données spécifiques

Il peut y avoir des différences sur les détails, ainsi qu'une pléthore d'obscurcissement et de destruction supplémentaires qui pourraient être déployés, mais la stratégie est toujours la même.

Comment stopper le ransomware ?

La plupart des recommandations de sécurité impliquent le traitement des étapes 1 et 5 ci-dessus dans la séquence d'attaque. Pour l'étape 1, il est recommandé d'utiliser le filtrage de courrier électronique et la formation des utilisateurs pour empêcher ces derniers de cliquer sur des téléchargements suspects ou des liens Web. Bien qu'il s'agisse d'une bonne idée, cette mesure est affreusement inadéquate de toute évidence, sinon les attaques de ransomware ne continueraient pas à augmenter en fréquence. Les hackers deviennent progressivement plus futés et il devient de plus en plus difficile de distinguer les e-mails malveillants de ceux légitimes. De plus, il existe d'autres moyens de leurrer les utilisateurs,

comme compromettre les sites Web que les utilisateurs ciblés pourraient fréquemment visiter (une pratique connue sous le nom de trou d'eau).

Pour l'étape 5, il est recommandé d'avoir un robuste plan de sauvegarde et de récupération, afin de pouvoir facilement formater et restaurer un système s'il venait à être compromis et chiffré. Il s'agit d'une excellente recommandation, car elle est profitable même dans des cas de reprise après sinistre. Mais 1) les ransomwares deviennent de plus en plus sophistiqués et peuvent également cibler même vos copies de sauvegarde, et 2) avez-vous déjà essayé de restaurer un seul système, sans parler d'un contrôleur de domaine ou de centaines de systèmes au sein d'une entreprise ? Ce n'est pas seulement un cauchemar, mais cela peut prendre des semaines et certaines données seront inéluctablement perdues.

Zscaler Workload Segmentation se concentre sur les étapes 2 à 4. Si la charge malveillante ne peut pas contacter son serveur de commande et de contrôle (C&C) ou n'est pas en mesure de surveiller le réseau ou de se propager vers d'autres systèmes, l'attaque peut être déjouée dans son déroulement, ou du moins sa portée peut être réduite.

C'est là que l'approche Zero Trust du trafic est-ouest est la plus efficace. Zero trust signifie que seules les entités autorisées, telles que les applications, les utilisateurs et les appareils, sont en mesure de communiquer avec d'autres entités autorisées. L'hypothèse est que le réseau en soi ainsi que ses adresses/ports/protocoles sont intrinsèquement non sécurisés. La confiance est établie sur la base du « qui » communique, et pas seulement du « comment » ils communiquent.

La plupart des réseaux sont excessivement permissifs lorsqu'il s'agit d'autoriser les systèmes d'un même réseau à communiquer entre eux. Au moins 87 % des voies d'accès autorisées dans la plupart des réseaux d'entreprise sont soit inexploitées, soit non nécessaires. Cette permissivité excessive existe parce que les pare-feux traditionnels n'offrent pas la granularité nécessaire pour restreindre réellement le trafic en fonction des entités qui utilisent ces connexions. Par exemple, supposons que vous utilisez Active Directory et que vous souhaitez que vos contrôleurs de domaine et vos clients communiquent sur les ports 88 et 135. Avec un pare-feu traditionnel, le mieux que vous puissiez faire est de restreindre le trafic en fonction des adresses IP de votre réseau et de ces ports. Tout élément de code malveillant pourrait toujours utiliser ces mêmes adresses et ports pour communiquer avec le contrôleur aux fins de collecte d'informations ou même d'exploitation.

Les NGFW, ou pare-feux de nouvelle génération, sont en mesure d'inspecter le trafic pour voir s'il est conforme aux attentes, mais les logiciels malveillants peuvent facilement contourner ce problème en utilisant simplement la syntaxe que le NGFW considère comme « légitime ». Qui plus est, la connexion

doit réellement se produire pour que le NGFW puisse identifier tout ce qui est suspect, et dans certains exploits, au moment où la connexion est identifiée comme « mauvaise », les dommages ont déjà été subis. En outre, le déploiement des NGFW à chaque point d'étranglement entre les différents systèmes peut s'avérer exorbitant en termes de coût et générer un décalage important dans le réseau — qu'il s'agisse de réseaux physiques ou d'environnements cloud virtualisés.

Zscaler Workload Segmentation (ZWS) adopte une approche différente de la microsegmentation. La solution assure la sécurité du réseau sur la base de l'identité réelle des applications et des services qui communiquent. Les logiciels non autorisés ou malveillants sont privés de communication, même s'ils utilisent les mêmes adresses, ports et protocoles autorisés par un pare-feu traditionnel, et même s'ils utilisent la même syntaxe identifiée par l'inspection des paquets dans un NGFW.

L'utilisation de la microsegmentation basée sur l'identité au sein de votre réseau présente de nombreux autres avantages, notamment un déploiement plus facile (aucune modification de l'infrastructure n'est requise), une compression des politiques et une gestion plus facile (beaucoup moins de politiques sont nécessaires), des politiques automatiquement mises à l'échelle (car les politiques sont basées sur l'identité et non sur les adresses réseau) et une meilleure visibilité de votre réseau (une bonne compréhension de la manière dont les applications communiquent, et pas seulement les adresses). D'un point de vue strictement sécuritaire, la sécurité basée sur l'identité de ZWS aurait pu facilement empêcher un chargeur malveillant de télécharger des composants supplémentaires, d'utiliser même des logiciels légitimes déjà présents sur le système pour surveiller et cataloguer le réseau, et de se propager à d'autres systèmes à l'aide de techniques telles que RDP ou PSEXEC.

Freiner la séquence, neutraliser l'attaque

Apprendre aux utilisateurs à se défendre contre les attaques d'hameçonnage et disposer d'une stratégie de sauvegarde pour la récupération en cas de catastrophe sont de bonnes stratégies, mais à elles seules insuffisantes pour neutraliser les ransomwares. La majorité des étapes des attaques de ransomware impliquent des communications non autorisées de logiciels malveillants ou compromis. Les pare-feux traditionnels ne sont pas de taille, mais la segmentation ZWS basée sur l'identité empêchera efficacement les ransomwares d'itérer et de se propager dans votre environnement. Il est temps de se libérer de l'emprise des ransomwares.

Remarque : Zscaler Threat Library et Cloud Sandbox détecteront à la fois Ryuk et Conti. D'autres détails techniques sont disponibles ici.