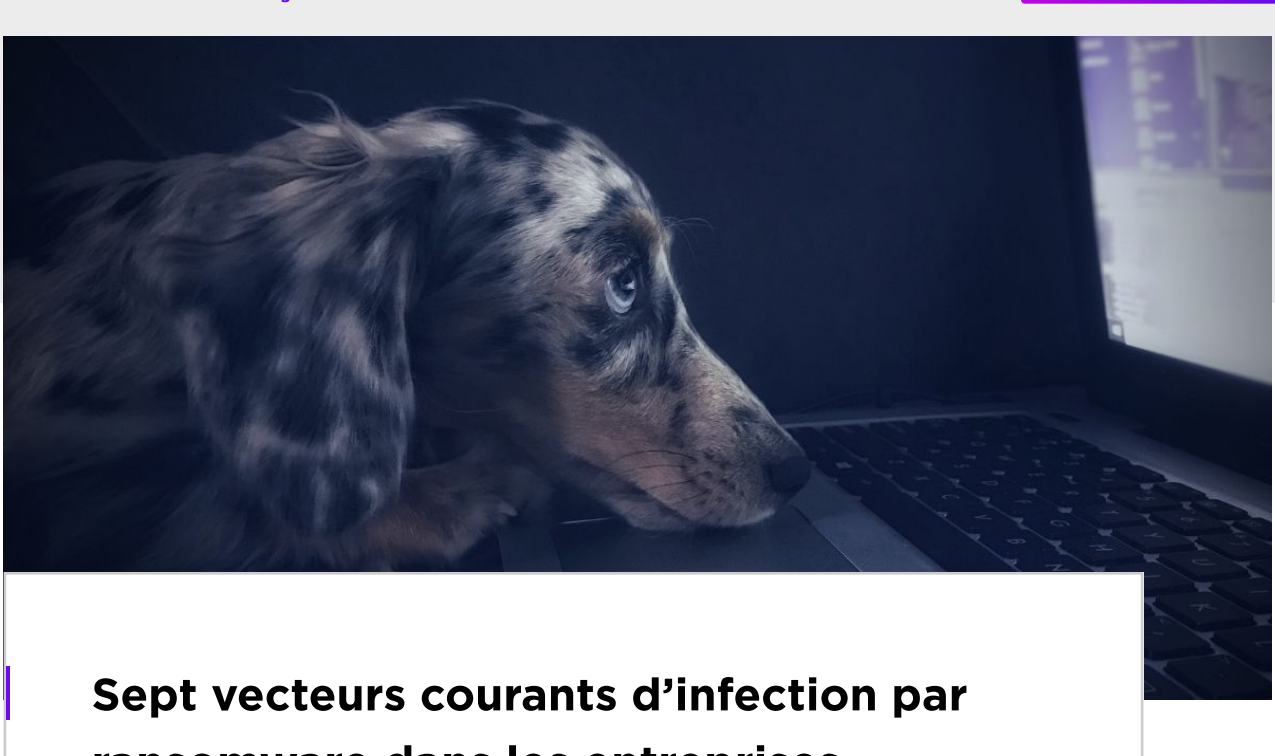


Sept vecteurs courants d’infection par ransomware dans les entreprises

mai 26, 2020
by SentinelOne

Si vous voulez éviter que votre entreprise ne devienne la prochaine victime d’une attaque, il est essentiel de comprendre comment un ransomware peut infecter un équipement et se propager dans un réseau. Comme le révèlent les dernières tendances, le risque de perte d’accès aux données, équipements et services est encore amplifié par l’émergence de cybercriminels dont le mode opératoire consiste désormais à exfiltrer des données et à menacer de les divulguer sur des sites publics si leurs victimes ne versent pas de rançon. Les auteurs de ransomware ont pris conscience de la précarité de leur ancien modèle de fonctionnement, en raison même de son succès : la médiatisation de leurs attaques a poussé les entreprises (du moins certaines d’entre elles) à investir dans des solutions de sauvegarde et de restauration. Mais ces technologies deviennent inutiles lorsque les cybercriminels utilisent vos informations clients et vos données d’entreprise sensibles comme une épée de Damoclès.

Après l’infection, le ransomware peut se propager à d’autres machines ou chiffrer les dossiers partagés sur le réseau de l’entreprise. Dans certains cas, il peut franchir les limites de l’entreprise pour infecter les chaînes logistiques, les clients et d’autres sociétés. D’ailleurs, certaines campagnes ont tout spécialement ciblé des fournisseurs de services managés (MSP) dans ce but. En matière de ransomware, mieux vaut prévenir que guérir. Comment ce malware destructeur s’y prend-il en règle générale pour infecter les équipements ?

1. Phishing et ingénierie sociale

La méthode la plus courante pour infecter initialement un endpoint par un ransomware reste l’envoi d’un e-mail de phishing. Les cybercriminels utilisent dans ces messages des informations de plus en plus ciblées, personnalisées et spécifiques pour gagner la confiance des destinataires et les inciter à ouvrir des pièces jointes ou à cliquer sur des liens pour télécharger des PDF malveillants et d’autres documents. Ces fichiers frauduleux sont parfois très difficiles à distinguer des fichiers normaux, les cybercriminels tirant parti par ailleurs d’un paramètre de configuration par défaut de Windows, qui masque les extensions de fichier. Par exemple, une pièce jointe peut apparaître sous le nom « nomdefichier.pdf », alors que l’affichage de l’extension complète révèle qu’il s’agit d’un exécutable, en l’occurrence « nomdefichier.pdf.exe ».

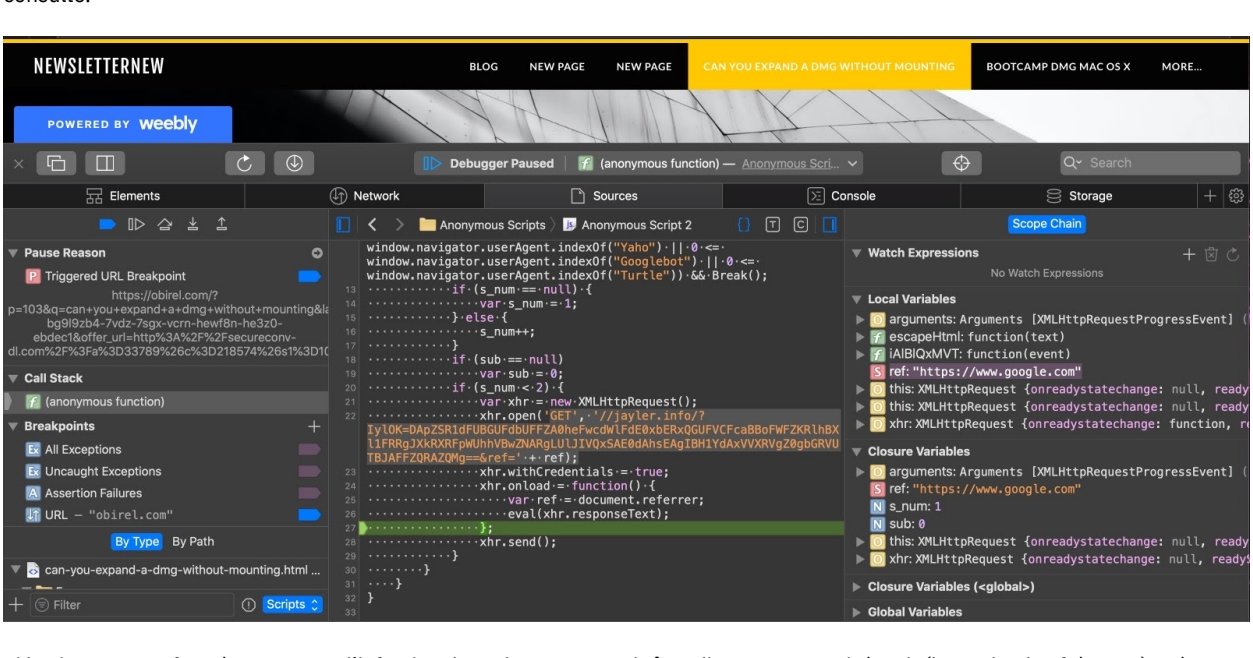
Voir aussi : Phishing | Les cibles les plus vulnérables

Les fichiers peuvent prendre la forme de formats standard comme des pièces jointes Microsoft Office, des fichiers PDF ou des scripts JavaScript. Un simple clic sur ces fichiers ou l’activation de macros permet au fichier malveillant de s’exécuter et de lancer le chiffrement des données sur l’ordinateur de la victime.

2. Sites Web compromis

Toutes les attaques par ransomware n’utilisent pas des e-mails comme vecteurs. Les sites Web compromis sont également une source de code malveillant. Il suffit que la victime accède au site en question, parfois l’un de ceux qu’elle consulte régulièrement, pour qu’elle se fasse piéger. L’internaute est redirigé vers une page qui l’invite à télécharger une nouvelle version d’un logiciel quelconque, par exemple un navigateur, un plug-in ou un lecteur multimédia.

Les redirections Web de ce genre sont extrêmement difficiles à détecter sans examiner le code sous-jacent de chaque site consulté.



Si le site est transformé en vecteur d’infection, le malware peut soit être directement activé, soit (le cas le plus fréquent) exécuter un programme d’installation qui télécharge et injecte le ransomware.

3. Publicités malveillantes et compromission du navigateur

S’il existe une vulnérabilité non corrigée sur le navigateur d’un utilisateur, ce dernier peut être victime d’une attaque par publicité malveillante. Par l’entremise de publicités couramment affichées sur des sites Web, les cybercriminels peuvent insérer du code malveillant qui télécharge le ransomware dès l’affichage de l’annonce. Même s’il s’agit d’un vecteur de ransomware moins répandu, il constitue néanmoins un danger dès lors qu’il n’exige pas l’exécution d’une quelconque action de la part de l’utilisateur, comme le téléchargement d’un fichier ou l’activation de macros.

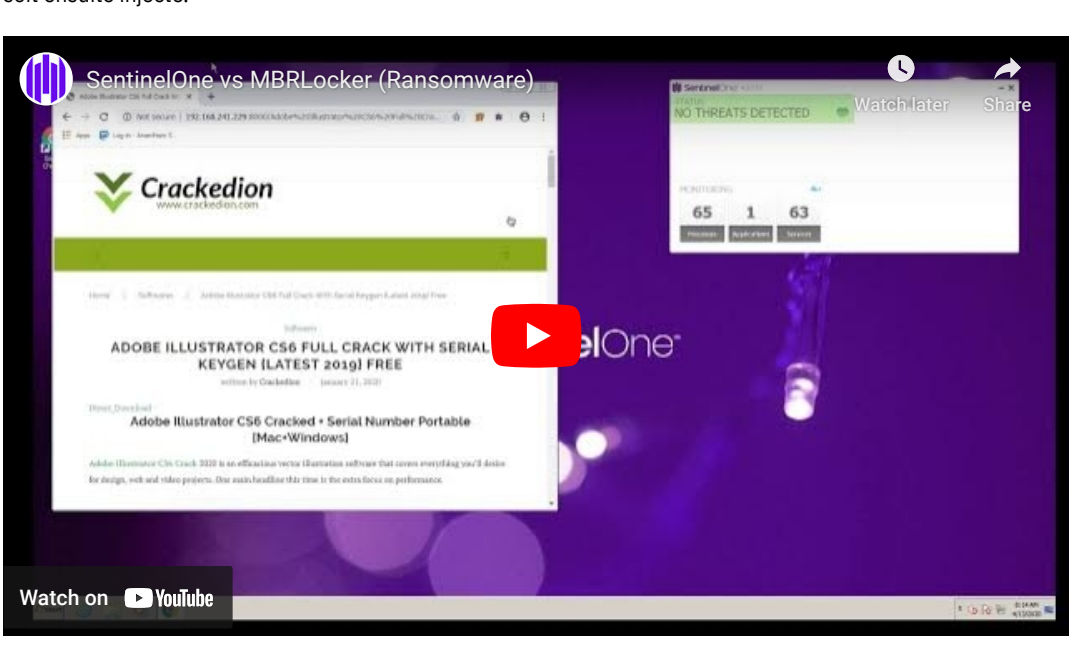
Voir aussi : Sécurité macOS | Comment les Mac se retrouvent-ils infectés par des malwares ?

4. Kits d’exploit distribuant un malware personnalisé

Angler, Neutrino et Nuclear sont des kits d’exploit régulièrement utilisés dans les attaques par ransomware. Il s’agit de kits d’outils malveillants incluant des exploits déjà écrits et conçus pour cibler des vulnérabilités des modules d’extension de navigateur, par exemple Java et Adobe Flash. Microsoft Internet Explorer et Microsoft Silverlight sont également régulièrement ciblés. Des ransomwares comme Locky et CryptoWall ont été distribués via des kits d’exploit sur des sites piégés et par l’intermédiaire de campagnes d’attaques utilisant des publicités malveillantes.

5. Téléchargement d’applications et fichiers infectés

Tout fichier ou application susceptible d’être téléchargé peut également être utilisé dans le cadre d’une attaque par ransomware. Les logiciels piratés hébergés sur les sites de partage de fichiers illégaux sont des portes ouvertes à la compromission ; ils sont d’ailleurs, plus souvent qu’à leur tour, truffés de malwares. C’est la voie que semblent emprunter, par exemple, les récentes variantes de MBRLocker, qui ont fait beaucoup parler d’elles. Il arrive aussi que les cyberpirates exploitent des sites Web légitimes pour distribuer un fichier exécutable infecté. Il suffit que la victime télécharge le fichier ou l’application pour que le ransomware soit ensuite injecté.



6. Applications de messagerie

Dans des applications de messagerie comme WhatsApp et Facebook Messenger, le ransomware peut prendre la forme d’un fichier graphique SVG pour charger un fichier qui contourne les filtres traditionnels des extensions. Comme SVG est basé sur XML, les cybercriminels sont en mesure d’incorporer le contenu de leur choix. Dès que la victime accède au fichier image infecté, ce dernier la redirige vers un site en apparence légitime. Après le chargement, la victime est invitée à accepter une installation qui, si elle est menée à terme, distribue la charge active et passe aux contacts de la victime pour continuer à se propager.

Voir aussi : Dissimulation de code au sein d’images : exploitation de la stéganographie par les malwares

7. Attaque par force brute via RDP

Les cybercriminels utilisent des ransomwares comme SamSam pour compromettre directement les endpoints à l’aide d’une attaque par force brute via des serveurs RDP (Remote Desktop Protocol) exposés à Internet. RDP permet aux administrateurs IT d’accéder à l’équipement d’un utilisateur à distance pour en prendre le contrôle, mais il offre aussi un moyen pour les cyberpirates d’exploiter ce protocole à des fins malveillantes.

Voir aussi : Sept techniques pour voler les mots de passe

Les cyberpirates peuvent rechercher les machines vulnérables à l’aide d’outils tels que Shodan et des analyseurs de ports comme Nmap et Zenmap. Une fois les ordinateurs cibles identifiés, ils tentent d’y accéder au moyen d’une attaque par force brute destinée à en découvrir le mot de passe administrateur. Une combinaison d’identifiants par défaut ou de mots de passe faibles et d’outils de décodage des mots de passe open source tels que Aircrack-ng, John The Ripper et DaveGrohl leur permet d’atteindre cet objectif. Une fois connecté en tant qu’administrateur approuvé, le cyberpirate dispose d’un contrôle total sur la machine et est en mesure d’injecter un ransomware et de chiffrer les données. Dans certains cas, il peut également désactiver la protection des endpoints, supprimer des sauvegardes afin d’accroître la probabilité d’un paiement ou basculer vers d’autres systèmes pour atteindre d’autres objectifs.

Conclusion

Le ransomware continue d’évoluer et le Ransomware-as-a-Service (RaaS) gagne en popularité. Les auteurs de malwares vendent aux cybercriminels des ransomwares créés « sur mesure » en échange d’un pourcentage des gains. L’acheteur du service décide des cibles et des méthodes de distribution. Cette répartition des tâches et des risques conduit à l’apparition de malwares de plus en plus ciblés et de nouvelles méthodes de distribution et, au bout du compte, à une multiplication des attaques par ransomware.

Au vu de ces diverses tendances, et de l’émergence des tentatives d’extorsion liées aux fuites de données, les entreprises doivent impérativement investir dans des solutions de protection des endpoints et des réseaux, et empêcher dès le départ toute compromission au moyen de moteurs d’analyse comportementale pilotés par intelligence artificielle qui ne se limitent pas à analyser la réputation et ne dépendent pas de la connectivité au cloud. Si vous voulez découvrir comment SentinelOne peut vous aider à protéger votre entreprise contre le ransomware et d’autres menaces, contactez-nous sans attendre ou demandez une démonstration gratuite.

Nous tenons à remercier Daniel Card et Chris Roberts pour leur assistance lors de la rédaction de cet article de blog.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Rapport d’enquête 2020 de Verizon sur les compromissions de données – Guide de référence à destination des RSSI
- Faire entrer l’identité dans l’ère du XDR
- Six idées reçues dont doivent se méfier les conseils d’administration des entreprises