solarwinds msp

eBOOK

5 cybermenaces capables de contourner les antivirus traditionnels

Table des matières

INTRODUCTION **3**

1. Logiciels malveillants polymorphes 4
2. Documents infiltrés 4
3. Téléchargements furtifs 5
4. Attaques sans fichiers 5
5. Logiciels malveillants dissimulés 6

Comment SolarWinds peut vous aider 7

5 cybermenaces capables de contourner les antivirus traditionnels

Le premier virus informatique a vu le jour en 1971 sous le nom de « Creeper ». Développé dans un contexte universitaire, son objectif était de démontrer la capacité d'un fichier à se déplacer sur un réseau. Six mois ont été nécessaires pour développer un programme antivirus efficace, appelé Reaper[1]. Cette période a marqué le premier décalage entre menace et défense.

Depuis, les professionnels de la sécurité et les programmeurs ne cessent de rattraper leur retard. Ils détectent les menaces, mettent à jour leurs défenses et répètent ce processus autant de fois que nécessaire.

La plupart des antivirus (AV) traditionnels reposent sur des signatures : lorsqu'un logiciel malveillant est découvert, une signature décrivant ses caractéristiques est générée, ajoutée à une base de données, qui est ensuite transmise à votre antivirus.. Si un fichier correspondant à une signature est détecté sur votre ordinateur, il est mis en quarantaine et/ou supprimé. En décembre 2018, 350 000 nouvelles menaces étaient découvertes par jour[2]. Les antivirus basés sur des signatures peinent à suivre ce rythme alarmant, et laissent des appareils vulnérables.

Au fil du temps, de nouvelles défenses voient le jour. Mais les cybercriminels adaptent leurs méthodes en conséquence. Les logiciels malveillants sont aujourd'hui capables d'exploiter les vulnérabilités, mais surtout de contourner les défenses des antivirus. Examinons les cinq types d'attaques capables de déjouer un antivirus classique.

1. « All About Creeper, the First Virus in History » (Tout ce qu'il faut savoir sur Creeper, premier virus de l'histoire), Softonic. en.softonic.com/articles/all-about-creeper-the-first-virus-in-history (en anglais, consulté en avril 2019).
2. « Malware » (Logiciels malveillants), AV-TEST. av-test.org/en/statistics/malware/ (en anglais, consulté en avril 2019).

1. LOGICIELS MALVEILLANTS POLYMORPHES

Comme nous l'avons vu en introduction, la plupart des antivirus traditionnels reposent sur un système de signatures. Ils comparent les fichiers avec une base de données de menaces connues, dénommées « signatures ».

Ce système de protection présente des inconvénients. Tout d'abord, l'utilisateur doit disposer de la liste de signatures la plus récente, ce qui l'oblige à effectuer des mises à jour régulières. S'il n'effectue pas ces mises à jour, il se retrouve sans défense face aux nouveaux fichiers malveillants. Ensuite, ce système agit par « réaction » : pour qu'une signature soit transmise à une base d'utilisateurs, il faut qu'elle soit au préalable découverte par les fournisseurs d'antivirus. Or, les logiciels malveillants mettent souvent en œuvre divers moyens pour éviter d'être détectés.

L'inconvénient majeur est le décalage observé en matière de protection, qu'il soit mesuré en temps ou en connaissances. Les logiciels malveillants polymorphes ont été conçus pour exploiter cette faille. S'ils sont détectés par un antivirus, ils se régénèrent en utilisant de nouvelles caractéristiques sans lien avec les signatures connues. Un antivirus basé sur des signatures peut alors difficilement stopper l'infection. Par ailleurs, environ 350 000 nouvelles variantes de programmes malveillants sont créées chaque jour[3]. Face à un tel nombre, les utilisateurs munis d'un antivirus basé sur des signatures rattrapent continuellement leur retard.

2. DOCUMENTS INFILTRÉS

Pour compromettre un système, les cybercriminels exploitent souvent les failles présentes dans différents formats de documents. En général, ils y intègrent du code ou des scripts, qu'ils parviennent à dissimuler. Le document piraté semble inoffensif même pour un œil averti. Il passe à travers les mailles du filet de l'antivirus, puisque ce dernier analyse le document initial et non le code ou le script une fois qu'il est exécuté. L'attaque se déroule alors en arrière-plan, sans que l'utilisateur le sache.

Les cybercriminels utilisent des fichiers Adobe® PDF contenant du JavaScript® pour exécuter des commandes du système d'exploitation, ou téléchargent des exécutables pour compromettre les périphériques et les réseaux auxquels ils ont accès. Ils ont souvent recours à des scripts intégrés pour exécuter des commandes PowerShell®. PowerShell étant intégré dans le système d'exploitation Windows®, ces attaques peuvent endommager les points de terminaison, voire des réseaux entiers. Les PDF ne sont pas les seuls types de fichiers vulnérables : les documents XML, HTML et Office® dissimulent souvent des scripts malveillants. Un antivirus basé sur la comparaison de signatures de fichiers exécutables ne détectera pas les documents infiltrés, car il analysera uniquement le document initial, et non le code malveillant exécuté par le document.

3. « Malware » (Logiciels malveillants), AV-TEST. av-test.org/en/statistics/malware/ (en anglais, consulté en avril 2019).

3. TÉLÉCHARGEMENTS FURTIFS

Les téléchargements furtifs (ou « drive-by downloads ») sont des fichiers téléchargés sur un point de terminaison à l'insu de l'utilisateur et de l'antivirus, en exploitant les vulnérabilités d'un navigateur ou d'une extension de navigateur. Ces téléchargements peuvent provenir d'un site Web légitime contenant un script ou un service d'annonces compromis, ou d'un site Web malveillant spécialement conçu pour livrer l'attaque. L'opération commence par un message de phishing, une pièce jointe ou un lien contextuel dissimulé pour diriger les utilisateurs vers un site Web. Les cybercriminels tirent ensuite parti des exploits des navigateurs ou des plug-ins pour télécharger des logiciels malveillants et mener leur action, qu'il s'agisse d'installer un cryptomineur, un cheval de Troie ou un ransomware. En octobre 2017, la ville de Issaquah dans l'État de Washington a été touchée par une attaque de ransomware qui a interrompu les services de la ville pendant quatre jours[4]. Tout a commencé par un téléchargement furtif, initié par un employé ayant ouvert un fichier PDF malveillant sur un site Web.

4. ATTAQUES SANS FICHIERS

La plupart des antivirus inspectent les fichiers écrits sur les périphériques. Si aucun fichier n'est déposé, impossible pour l'antivirus de détecter le comportement malveillant.

Les attaques sans fichiers se produisent sans installer de charge utile réelle sur un système, ce qui les rend extrêmement difficiles à détecter. Elles sont généralement exécutées dans la mémoire du point de terminaison, et utilisent PowerShell, rundll32.exe ou d'autres ressources système intégrées pour infecter les ordinateurs.

Les attaques sans fichiers commencent souvent par des documents ou des scripts malveillants sur un site Web, mais elles peuvent avoir recours à bien d'autres stratagèmes pour infecter un ordinateur. Par exemple, lorsqu'un point de terminaison active le protocole RDP (Remote Desktop Protocol), il laisse ouvert un port d'écoute qui peut permettre à un utilisateur de se connecter et de lancer des processus nuisibles, tels que le téléchargement de logiciels malveillants basés sur des fichiers, la modification du registre, ou le vol des données.

Comme si ce n'était pas assez effrayant, SentinelOne a constaté une augmentation de 91 % des attaques de logiciels malveillants sans fichiers au cours du premier semestre 2018[5]. Face à une telle progression, les entreprises doivent aller au-delà de la détection basée sur les fichiers pour mieux protéger leurs actifs et leurs données.

4. « How a Drive-by Download Attack Locked Down Entire City for 4 Days » (Comment un téléchargement furtif est parvenu à bloquer une ville entière pendant 4 jours), The Hacker News. thehackernews.com/2017/10/drive-by-download-ransomware.html (en anglais, consulté en avril 2019).
5. « Fileless Malware Attacks | How They Can Be Detected and Mitigated » (Attaques sans fichiers | Comment les détecter et les corriger), SentinelOne. sentinelone.com/blog/fileless-malware-attacks-can-detected-mitigated/ (en anglais, consulté en avril 2019).

5. LOGICIELS MALVEILLANTS DISSIMULÉS

Nous avons précédemment indiqué que les professionnels de la sécurité et les chercheurs essayaient constamment de « rattraper » les cybercriminels. Les fournisseurs d'antivirus emploient divers moyens pour découvrir les logiciels malveillants. Une méthode courante consiste à exécuter des fichiers dans des environnements de test (sandbox) et à détecter les comportements malveillants. Une autre consiste à rechercher dans le code les signes d'intention malveillante.

Les cybercriminels ont trouvé des solutions pour contourner ces méthodes. De la même manière que les professionnels de la sécurité mettent en place des moyens de défense pour préserver leurs données et leurs actifs, les pirates informatiques disposent d'astuces pour protéger le contenu nuisible d'un logiciel malveillant.

Les nouveaux malwares sont par exemple capables de détecter les environnements de test, où ils restent inoffensifs, pour finalement livrer leurs attaques dans les environnements en production. Un antivirus ne peut donc pas les détecter en amont.

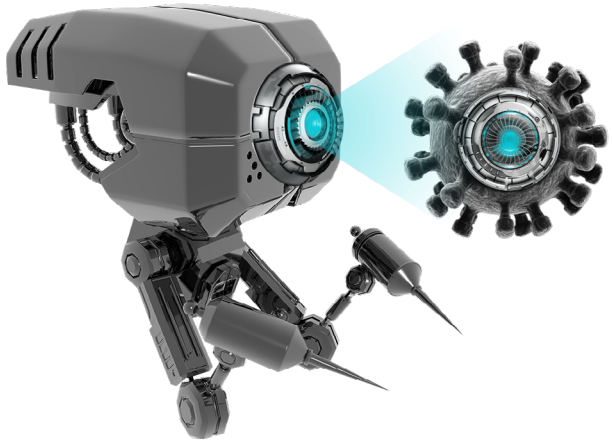
Une autre solution consiste à utiliser des « packers ». Le fichier malveillant est alors chiffré ou compressé pour empêcher toute personne de voir son contenu. Les cybercriminels peuvent également insérer du code malveillant dans du code légitime afin de le dissimuler.

Ces techniques empêchent les chercheurs en sécurité de détecter (et de comprendre) les fichiers malveillants. D'autant plus s'ils utilisent un antivirus basé sur des analyses heuristiques dans un environnement de test.

COMMENT SOLARWINDS PEUT VOUS AIDER

Pour contrer les menaces actuelles, les fournisseurs de services gérés doivent adopter une sécurité multicouche. Superposer les contrôles de sécurité est la clé pour réduire les risques d'attaques. SolarWinds MSP propose deux plateformes de supervision et de gestion à distance, SolarWinds® RMM et SolarWinds N-central®, pour vous aider à fournir plusieurs couches de protection à vos clients. En complément de l'antivirus, elles vous donnent accès à des fonctionnalités de protection Web pour détecter les liens malveillants, de protection de la messagerie pour empêcher le spam et les tentatives de phishing, de gestion des mises à jour pour corriger les vulnérabilités du système d'exploitation et des logiciels tiers. Si malgré cela, une attaque parvient à déjouer les systèmes de protection, la sauvegarde et la récupération intégrées vous permettront de restaurer vos fichiers ou vos systèmes.

Nos deux plateformes proposent également la fonctionnalité SolarWinds Endpoint Detection and Response (EDR), basée sur la technologie SentinelOne®. La fonction SolarWinds EDR est conçue pour prévenir, détecter et corriger les cybermenaces en constante évolution sur les points de terminaison des clients. Elle surpasse les antivirus classiques grâce à une approche sans signature (nul besoin d'attendre les analyses récurrentes ou la mise à jour des définitions de signatures). De plus, en cas d'attaque, EDR peut prendre des mesures pour contenir la menace, contrer ses effets et restaurer automatiquement le point de terminaison ou les fichiers compromis à un état antérieur stable.



*Pour en savoir plus, consultez le site **solarwindsmsp.com/fr***

SolarWinds est un acteur majeur dans l'offre de logiciels de gestion d'infrastructures informatiques performants et abordables. Nos produits permettent aux organisations du monde entier, quels que soient leur type, leur taille et la complexité de leurs infrastructures, de superviser et de gérer les performances de leurs environnements sur site, dans le Cloud ou hybrides. Nous travaillons en permanence avec tous les types de spécialistes des technologies — professionnels des opérations informatiques, professionnels DevOps, fournisseurs de services gérés (MSP) — afin de comprendre les défis auxquels ils font face pour maintenir la disponibilité et les performances de leurs systèmes à un niveau élevé. Destiné aux MSP, le portefeuille de produits SolarWinds MSP propose des solutions de gestion de services informatiques évolutives, fondées sur une sécurité multicouche, une intelligence collective et une automatisation intelligente. Ces produits sont conçus pour permettre aux MSP d'offrir des services informatiques externalisés très efficaces à leurs PME clientes, et de mieux gérer leurs propres activités.