

Protection de la mémoire

- Brief technique

Techniques de détection multi-niveaux :

1. Machine Learning

2. HyperDetect

3. Sandbox Analyzer

4. Protection de la mémoire

5. Process Inspector

Présentation

Dans le paysage actuel de la cybersécurité, les cybercriminels réalisent régulièrement des tests et modifient fréquemment leurs techniques d'attaques, rendant les entreprises plus vulnérables aux incidents et épidémies de malwares, aux interruptions d'activité et aux violations de données. La plateforme Bitdefender GravityZone Endpoint Security protège les endpoints contre l'ensemble des cyberattaques sophistiquées avec une grande efficacité, un faible impact pour l'utilisateur final, tout en limitant la charge de travail des administrateurs. Elle est composée de multiples couches de protection afin de bloquer les activités malveillantes les plus avancées. Chaque couche de sécurité est conçue pour stopper certains types précis de menaces, outils ou techniques, assurant ainsi une protection à plusieurs niveaux contre les cyberattaques. La protection de la mémoire de Bitdefender est intégrée à la plateforme GravityZone Endpoint Security. Elle assure une protection contre les exploits connus et inconnus qui ciblent les navigateurs Web et les vulnérabilités d'applications lors de leur exécution.

Phase de détection	Type de technologie	Types de menaces détectées
À l'exécution	Exploits	Attaques par phishing, malvertising, drive-by downloads, attaques sans fichier, attaques par ingénierie sociale, vulnérabilités des applications et des systèmes d'exploitation, élévations des privilèges, injections de code

Intérêt de la protection de la mémoire

Un exploit est un type d'attaque qui tire profit d'une vulnérabilité afin de compromettre un endpoint et y injecter un malware. De nombreuses épidémies de malwares, notamment celles de type ransomwares, sont diffusées via des exploits. Les cybercriminels utilisent des kits d'exploits disponibles sur les marchés noirs afin de diffuser des attaques et d'identifier de nouvelles victimes. Un kit d'exploit est un ensemble d'outils qui automatise l'exploitation des vulnérabilités présentes dans les applications les plus connues, telles que les navigateurs Web, les applications Microsoft Office ou encore Adobe Reader. Lorsque le navigateur d'une potentielle victime se connecte à un site Web hébergeant un kit d'exploit, ce dernier sonde le système de l'utilisateur et extrait certaines informations, telles que la version du système d'exploitation et le type de navigateur, pour détecter des vulnérabilités à exploiter. Une fois que le cybercriminel a identifié une vulnérabilité, une charge active malveillante est diffusée sur le système et l'attaque est lancée.

Bien que de nombreuses vulnérabilités, anciennes comme nouvelles, existent toujours au sein d'applications, les pirates n'utilisent qu'un petit nombre de techniques d'exploitation. La technologie de protection de la mémoire de Bitdefender protège les entreprises contre ces techniques d'exploitation, empêchant ainsi les attaques aussi bien connues qu'inconnues.



La tristement célèbre attaque Wannacry qui a touché plus de 150 000 endpoints dans le monde en 24 heures a été rendue possible par un exploit de mémoire dénommé EternalBlue. Cela a rendu l'attaque particulièrement difficile à détecter par les systèmes de sécurité traditionnels pour endpoints.

Caractéristiques

- Protège les applications standard des utilisateurs, notamment : les navigateurs Web et leurs composants, les lecteurs PDF, les applications Microsoft.
- Intègre plusieurs mécanismes avancés de détection des exploits pour protéger contre les contournements de la sécurité des systèmes d'exploitation par les malwares et contre la corruption de la mémoire : Caller check, Stack pivot, exécution de la mémoire récemment allouée, Executable stack, Return to stack, Thread vers la mémoire récemment allouée, action Shellcode, écrasement de pointeur de fonction Flash.

Avantages

- Détecte les attaques avancées en amont et empêche les violations de données, réduit les coûts et les efforts en réponse aux incidents.
- Réduit les efforts de recherche des menaces.
- Améliore le taux de détection des menaces Zero-day, les attaques par phishing, le malvertising, le drive-by Download, les attaques sans fichier, les attaques par ingénierie sociale, les élévations des privilèges et l'injection de code.
- Est intégrée à l'agent de sécurité unifié pour endpoint GravityZone et à la plateforme centralisée d'administration, réduisant ainsi la charge de travail des administrateurs. Ces derniers n'ont ainsi pas à déployer plusieurs solutions de sécurité pour endpoints.



Bitdefender est une entreprise mondiale de sécurité qui développe des solutions de cybersécurité de pointe et qui protège plus de 500 millions d'utilisateurs dans plus de 150 pays. Depuis 2001, Bitdefender développe des technologies régulièrement récompensées, pour les marchés des entreprises et des particuliers, et est un fournisseur recommandé pour sécuriser les infrastructures hybrides et protéger les endpoints. Grâce à ses équipes R&D, ses alliances et partenariats, Bitdefender est reconnu pour être un éditeur innovant, proposant des solutions de sécurité fiables et efficaces, sur lesquelles vous pouvez compter. Plus d'informations sur www.bitdefender.fr

Tous droits réservés. © 2018 Bitdefender. Toutes les marques, noms commerciaux et produits cités dans ce document sont la propriété exclusive de leurs détenteurs respectifs. Pour plus d'informations, veuillez consulter www.bitdefender.fr/business

