Les cybercriminels exploitent l’enthousiasme suscité par ChatGPT pour propager des malwares.

Alors que les exploits de vulnérabilités se multiplient, les chercheurs en sécurité de Palo Alto Networks ont observé une recrudescence des tentatives d’imitation de ChatGPT par le biais de domaines squattés. Les techniques traditionnelles de malware profitent de plus en plus de l’intérêt pour ChatGPT et d’autres programmes d’IA générative. La popularité de ChatGPT a également entraîné l’apparition de grayware, qui peut causer des problèmes ou porter atteinte à la vie privée. Pour se prémunir contre les attaques de ces logiciels, les entreprises doivent continuer à utiliser les meilleures pratiques de défense en profondeur. Le nombre de tentatives d’exploitation des vulnérabilités a également augmenté, ce qui peut être attribué à l’augmentation des tentatives d’exploitation des vulnérabilités Log4j et Realtek. Les PDF contenant des pièces jointes malveillantes restent un vecteur d’attaque initial très prisé des attaquants pour diffuser des logiciels malveillants. Les variantes de Ramnit ont été la famille de logiciels malveillants la plus couramment déployée l’année dernière. En outre, Palo Alto Networks a observé que le nombre moyen d’attaques par client dans le secteur de la fabrication, des services publics et de l’énergie a augmenté de 238 % l’année dernière, et les logiciels malveillants ciblant Linux sont en hausse. Les acteurs malveillants utilisent des PDF pour tromper les utilisateurs grâce à des techniques d’ingénierie sociale, en utilisant souvent des lignes d’objet séduisantes, des visuels attrayants ou un contenu trompeur

pour amener les utilisateurs à ouvrir un fichier PDF. Les attaquants cherchent de nouvelles opportunités dans les charges de travail cloud et les terminaux IoT qui fonctionnent avec des systèmes d'exploitation de type Unix. Les entreprises doivent mettre en œuvre un programme complet de gestion des correctifs comprenant des évaluations régulières, des analyses et une hiérarchisation en fonction des niveaux de risque pour s'assurer que les vulnérabilités anciennes et nouvelles sont corrigées régulièrement. Les contrôles de sécurité qui défendent contre les attaques traditionnelles seront une première ligne de défense importante contre toutes les attaques liées à l'IA qui se développent à l'avenir. Concentrez-vous sur la correction des vulnérabilités critiques qui pourraient avoir l'impact le plus important sur les systèmes et les données de l'organisation.

Source : www.lemondeinformatique.fr

→ Accéder à CHAT GPT en cliquant dessus