Sécurité des systèmes embarqués

Trend Micro mobilise les hackers éthiques à l'échelle mondiale pour identifier les vulnérabilités des véhicules connectés

Pour renforcer la cybersécurité dans ce domaine stratégique,
la Zero Day Initiative crée un bug bounty dédié : le Pwn2Own Automotive.

Rueil-Malmaison, le 30 janvier 2022 – Trend Micro Incorporated (TYO : 4704 ; TSE : 4704), entreprise japonaise parmi les leaders mondiaux en matière de sécurité numérique, annonce que le concours de bug bounty 'Pwn2Own' organisé par la Zero Day Initiative (ZDI), pour laquelle il est contributeur majeur, lancera en 2024 un rendez-vous destiné à améliorer la sécurité des véhicules connectés. La compétition 'Pwn2Own Automotive' se tiendra à l'Automotive World de Tokyo, en janvier 2024.

« Aujourd'hui, une voiture n'est pas seulement un moteur et quatre roues. Les véhicules que nous utilisons s'appuient sur des systèmes et des composants qui forment une informatique embarquée puissante mais qui étendent également la surface d'attaque », commente Brian Gorenc, senior director of vulnerability research et responsable de la ZDI. *« Grâce à sa filiale VicOne, spécialisée dans la cybersécurité automobile, et à Pwn2Own, Trend Micro protège un pan majeur de ce monde connecté. »*

Depuis sa création il y a 17 ans, Pwn2Own met au défi les meilleurs hackers du monde de trouver et d'exploiter les vulnérabilités de logiciels et de dispositifs largement utilisés au quotidien. Une initiative qui tend à identifier des failles avant que les acteurs de la menace ne les exploitent.

L'évènement de bug bounty 'Pwn2Own Automotive' a pour objectif de :

1. **Encourager et de faire avancer la recherche en matière de sécurité des véhicules connectés**, en soutenant financièrement les chercheurs engagés dans la publication de rapports couvrant les produits et plateformes nécessaires à la protection automobile.

2. **Lever le voile sur la surface d'attaque** en mettant en évidence les technologies critiques qui doivent être évaluées.

3. **Promouvoir la découverte de menaces complexes** en offrant un niveau de récompense plus élevé pour celles d'attaques multi-systèmes.

Au cours des dernières années, les systèmes automobiles ont pris une place majeure au sein de l'évènement Pwn2Own, grâce notamment au concours de Tesla. En 2019, une équipe a remporté le prix global Master of Pwn après avoir réussi à pirater une Tesla Model 3. Puis, en 2021, l'exploitation de deux autres bugs uniques dans le système d'info-divertissement de la voiture a été démontrée. Le constructeur de voitures électriques sera également présent en 2023 à Pwn2Own Vancouver en tant que sponsor et offrira une Model 3 aux potentiels participants qui découvriraient de nouvelles vulnérabilités au sein de son véhicule connecté.

#Cybersécurité #Connectedcars #Pwn2Own

À propos de Trend Micro

Trend Micro, un leader mondial de la cybersécurité, sécurise les échanges d'informations numériques. Fruit de décennies d'expérience en sécurité, de recherches sur les menaces et d'innovation, notre plateforme unifiée de cybersécurité protège 500 000 entreprises et des millions d'individus contre les risques associés aux réseaux, équipements, endpoints et au cloud.

Plateforme unifiée de cybersécurité, Trend Micro One déploie une ligne de défense sophistiquée contre les menaces et combine de nombreuses fonctionnalités comme l'XDR, le Zero Trust, le SASE… . Elle s'intègre avec de nombreux écosystèmes IT (AWS, Microsoft, Google…) et permet aux entreprises de comprendre et maîtriser leurs risques.

Les 7 000 collaborateurs de Trend Micro, présents sur 65 pays, aident les entreprises à simplifier et sécuriser leur univers interconnecté. TrendMicro.com

Pour plus d'informations sur les produits et services Trend Micro : www.trendmicro.com
Suivez-nous sur les réseaux sociaux :
http://www.twitter.com/TrendMicroFR
https://www.linkedin.com/company/trend-micro-europe/