Communiqué de Presse

AL'X COMMUNICATION - Véronique Loquet

Synacktiv triomphe à la compétition Pwn2Own 2024 de Tokyo, avec des démonstrations de hacking inédites sur véhicules connectés, et 2 attaques réussies sur la Tesla

L'équipe française de chercheurs en cybersécurité se hisse au sommet de la compétition et remporte plusieurs Prix lors du Pwn2Own Automobile, qui s'est tenu à la Conférence Automotive World à Tokyo du 24 au 26 janvier 2024.

Paris, le 29 janvier 2024 – L'équipe de hackers français de Synacktiv remporte la compétition Pwn2Own de Tokyo dédiée aux véhicules connectés. Cette nouvelle victoire s'ajoute à une liste impressionnante de succès pour Synacktiv, qui participe à la compétition Pwn2Own depuis 2020.

Organisé par Zero Day Initiative (ZDI) le concours de piratage Pwn2Own Automotive vise à sensibiliser le secteur automobile à la nécessité de renforcer la sécurité des véhicules connectés, et à encourager une collaboration proactive avec les chercheurs en cybersécurité à l'échelle mondiale. L'objectif est de révéler les vulnérabilités logicielles et systèmes des véhicules modernes et de favoriser la collaboration entre la communauté des hackers chercheurs en cybersécurité et l'industrie automobile.

Pwn2Own offre un programme de bug bounty qui permet à la fois aux constructeurs, tels que Tesla co-sponsor de l'édition, de tester et corriger les failles de sécurité de leurs véhicules et d'obtenir une vision approfondie des surfaces d'attaques, et aux hackers d'être récompensés en démontrant leur expertise pointue sur des attaques multi-systèmes.

Cette année, Synacktiv a relevé le défi avec des démonstrations de hacking inédites, en présentant 8 attaques :

- **4 attaques sur des chargeurs de véhicules électriques :** dans chaque cas, Synacktiv a pris le contrôle à distance de l'équipement, obtenant un accès complet.
- **1 attaque sur un équipement de type autoradio intelligent** (musique, caméra de recul, etc) **:** Synacktiv a pris le contrôle en connectant une simple clé USB.
- **1 attaque sur un système d'exploitation automobile :** Similaire à l'autoradio intelligent, Synacktiv a pris le contrôle en se connectant en USB.
- **2 attaques sur Tesla :** L'équipe a démontré la prise de contrôle à distance de plusieurs fonctionnalités du véhicule depuis le réseau mobile, obtenant des privilèges similaires à ceux acquis lors des compétitions de 2022 et une partie des privilèges de la compétition de 2023.

Une fois les failles révélées, les constructeurs ont 90 jours pour publier les correctifs de sécurité.

David Berard, chercheur en cybersécurité chez Synacktiv et participant au concours Pwn2Own de Tokyo, déclare : *« Nous participons à Pwn2Own avant tout pour le défi technique qu'il nous offre. Cela nous donne aussi l'opportunité de nous mesurer à d'autres professionnels du domaine. Les phases de préparation du concours, souvent longues, sont des moments enrichissants de travail en équipe. Les détails techniques complets des attaques sont généralement partagés par la suite lors de conférences internationales renommées. »*

Renaud Feil, co-fondateur et Président de Synacktiv, précise : *« Cette victoire au Pwn2Own est le résultat du dévouement continu de nos équipes envers l'innovation et la sécurité. Nous sommes fiers de repousser les limites de la cybersécurité et de contribuer à la protection des systèmes informatiques face aux menaces émergentes. »*

Sur cette édition 2024, Synacktiv remporte 450 000 dollars de récompense. L'entreprise affichait déjà un beau palmarès au Pwn2Own, puisque l'équipe française avait déjà remporté l'édition à Austin en 2021. En 2022, Synacktiv s'inscrivait dans l'histoire du concours en présentant pour la première fois l'exploitation réussie d'une faille sur un modèle Tesla lors de l'édition de Pwn2Own à Vancouver. Plus récemment, s'ajoutaient d'autres trophées à leur collection en remportant la première place de l'édition de Vancouver 2023, pour avoir réussi à compromettre la Tesla Model 3. Au final, l'équipe de Synacktiv avait remporté 530 000 $ et la Tesla Model 3, consolidant leur réputation de leaders incontestés dans le domaine de la cybersécurité offensive.

A propos de ZDI (Zero Day Initiative)

Zero Day Initiative (ZDI) organise le concours de piratage Pwn2Own, qui a lieu trois fois par an, au cours duquel des équipes de hackers peuvent remporter des prix en espèces ainsi que des logiciels et du matériel qu'ils ont réussi à exploiter. C'est un concours de hacking international de recherche de vulnérabilités logicielles, lancé en 2005 par TippingPoint. Le programme a été racheté par Trend Micro dans le cadre de l'acquisition de HP TippingPoint en 2015. ZDI achète diverses vulnérabilités logicielles à des chercheurs en cybersécurité, puis divulgue ces vulnérabilités à leurs fournisseurs d'origine pour qu'ils les corrigent avant de rendre ces informations publiques.

Le terme "zero-day" fait référence à la première fois, ou jour zéro, où un fournisseur prend connaissance d'une vulnérabilité dans un logiciel spécifique. Le programme a été lancé pour récompenser en espèces les pirates informatiques qui parviennent à trouver des exploits dans n'importe quel type de logiciel. ZDI a été créée en tant que programme tiers pour collecter et encourager la découverte de telles failles, tout en protégeant à la fois les chercheurs et les informations sensibles qui se cachent derrière ces vulnérabilités.

https://www.zerodayinitiative.com/about/

A propos de Synacktiv

Fondée en 2012 par deux experts en cybersécurité, ses principaux domaines d'expertise sont les tests d'intrusions, les audits de sécurité, la rétro-ingénierie, la recherche de vulnérabilités et la réponse à incidents.

Synacktiv participe à des projets sensibles de renommée mondiale. Elle développe de nombreux outils de sécurité offensifs dans le cadre de ses activités.

Synacktiv est agréée PASSI RGS et LPM (Prestataire d'Audit de la Sécurité des Systèmes d'Information) & CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information) par l'ANSSI. Labellisée

Cybersecurity Made In Europe par l'Alliance pour la Confiance Numérique (ACN), organisme certificateur autorisé par l’Autorité nationale des jeux (ANJ).

L’entreprise compte plus de 200 clients et emploie actuellement une équipe de plus de 150 experts en cybersécurité. Elle opère principalement depuis ses bureaux de Paris, Toulouse, Lyon, Lille et Rennes. Les équipes interviennent en France, en Europe et à l’international.

A une échelle nationale ou internationale, l’implication de Synacktiv au sein de la communauté cyber se traduit par la participation à de nombreux évènements (conférences, challenges, CTF) ainsi que la publication régulière d’alertes de sécurité ou d’articles.

Pour en savoir plus www.synacktiv.com