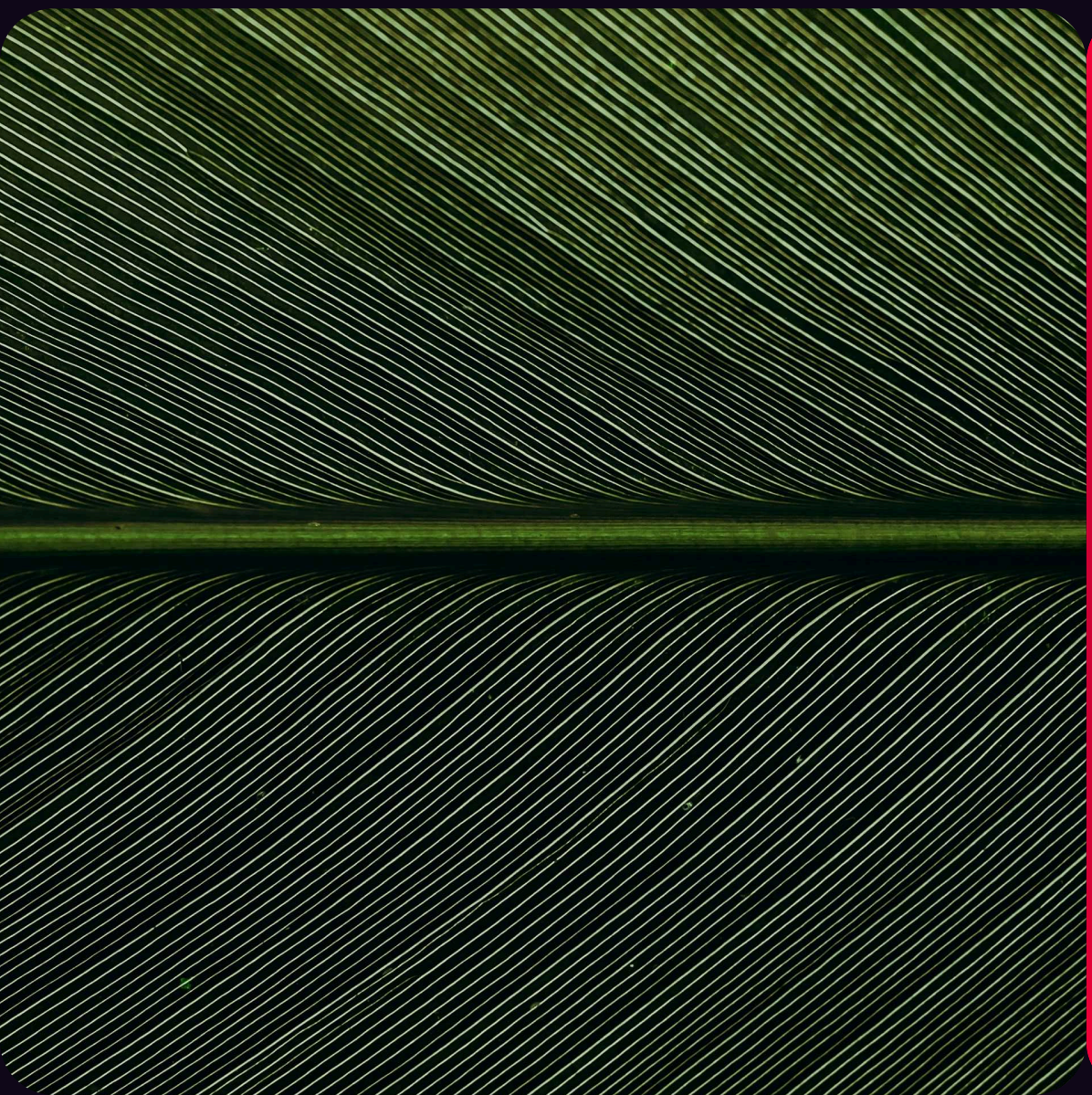
HADRIAN

ETUDE DE CAS

Leroy Merlin

TRAVAILLER AVEC L'ÉQUIPE DE SÉCURITÉ DE POUR
PRIORISER LES RISQUES EN ACCORD AVEC LEURS BESOINS

COMMERCE DE DÉTAIL MILAN, ITALIE



À propos de Leroy Merlin Italie

Leroy Merlin Italie est une filiale d'Adeo basée à Milan en Italie. En tant que détaillant de bricolage et de jardinage, Leroy Merlin dessert des pays en Europe, en Amérique du Sud et en Afrique.
Leroy Merlin compte 9000+ employés et un chiffre d'affaires annuel de 7,5 milliards d'euros. En 2020, Leroy Merlin a accéléré sa transformation numérique et cloud, développant des outils de shopping en ligne et une application.

CHIFFRE D'AFFAIRES ANNUEL

€ 7.5 Mrd

EMPLOYÉS

9000+

Défi

01 L'implémentation de sites web, d'applications mobiles et deméthodes de paiement numérique pour soutenir le commerce électronique entraîne l'expansion des surfaces d'attaque

02 Les clients effectuant des achats en ligne s'exposent à des comptes financiers compromis, à des informations personnellement identifiables (PII) et à des informations de carte de paiement

03 Les attaques entraînent une perte de revenus et de crédibilité pour les détaillants impactés

Solution

- Les outils de gestion de la surface d'attaque de Hadrian ont utilisé des collecteurs de données open source et des sources de données passives pour identifier des actifs auparavant inconnus de Leroy Merlin
- Les tests inter-actifs ont analysé des actifs à travers plusieurs fournisseurs de partage cloud et domaines et ont fourni des informations sur la manière dont ils étaient liés entre eux
- La technologie de fingerprinting a contextualisé les actifs en considérant la langue de l'application, la version et les vulnérabilités communes
- Les informations collectées ont été utilisées pour développer des chemins d'attaque uniques adaptés à la surface d'attaque de Leroy Merlin
- Hadrian a collaboré avec l'équipe de sécurité de Leroy Merlin pour prioriser les risques en accord avec leurs besoins

Résultat

Découverte d'actifs oubliés

Hadrian a déployé des outils de découverte d'actifs avec le but express d'identifier des actifs inconnus. Dans le cas de Leroy Merlin, Hadrian a utilisé des connaissances préalables sur la sécurité du commerce électronique pour déployer des outils ciblant les zones les plus susceptibles de contenir des actifs oubliés. Par exemple, les développeurs d'applications dans l'industrie du commerce électronique laissent souvent par accident des pages d'administration accessibles, permettant aux attaquants d'accéder à des fonctions d'administration sensibles. Hadrian a utilisé cette perspective et déployé un module de piratage conçu pour identifier des répertoires/pages d'administration oubliés.
Hadrian a pu identifier un point de terminaison vulnérable avec une page d'administration non surveillée.

FAUX POSITIFS ÉLIMINÉS

100+

RISQUES CRITIQUES TROUVÉS

3

“La plateforme de Hadrian identifie les vulnérabilités de manière plus approfondie que d'autres outils entièrement automatisés. Les informations fournies par Hadrian nous ont aidés à améliorer le blindage de nos systèmes. Excellentes perspectives. ”

CISO Leroy Merlin

Résultat

Développement de tests ciblés pour identifier les potentielles fuites de données

Lorsqu'un actif oublié ou non surveillé était identifié, Hadrian s'appuyait sur des informations open source et sa propre logique pour déterminer les chemins d'attaque pertinents. Les tests ciblés permettaient à Hadrian de valider la sécurité de Leroy Merlin sans surcharger l'infrastructure informatique.

Dans le cas de la page d'administration non surveillée, Hadrian a pu déterminer le test le plus efficace en considérant le contexte de l'application, spécifiquement son langage et son cadre. Hadrian a exécuté un test qui révélait souvent des risques sur des actifs avec des cadres similaires. Le test a révélé des identifiants pour les mots de passe de base de données et Google Cloud, ainsi que des cookies contenant des informations sensibles sur les utilisateurs.

La technologie d'événementiel génère des chemins d'attaque complexes

Hadrian a été construit en utilisant une technologie pilotée par les événements. Le test piloté par les événements signifie que les attaques longues et compliquées sont décomposées en composants plus petits qui peuvent être combinés dans différentes séquences, permettant une flexibilité. De plus, les informations recueillies lors des tests précédents déclenchent de nouveaux modules, résultant en une méthodologie de test qui est hautement adaptable. Les composants plus petits permettent à Hadrian de s'adapter au fur et à mesure que de nouvelles informations sont révélées.

Par exemple, lorsque Hadrian a découvert les cookies sur la page d'administration, cela a déclenché un outil de piratage. L'outil de piratage a utilisé les cookies pour accéder à des comptes contenant des informations sensibles sur l'entreprise et les clients.

Hadrian continuera à collecter des informations et à déployer des tests en réponse aux changements dans la surface d'attaque de Leroy Merlin.