

Étude de cas

juridique

RICOH
imagine. change.
imaginer. changer.

Une affaire de piratage de logiciel est résolue grâce à l'analyse approfondie effectuée par un expert des services judiciaires de Ricoh

Les techniques de criminalistique de pointe employées par l'expert de Ricoh ont permis de découvrir le document qui s'est avéré être la preuve irréfutable du piratage informatique que l'équipe d'enquête espérait trouver.

À PROPOS DU CLIENT

Le client est un important fabricant de logiciels à l'échelle internationale.

DÉFI

Le client a consacré environ sept mois à une enquête sur la source de nombreux CD contenant des versions contrefaites de ses produits logiciels. Un suspect a été identifié durant l'enquête et l'entreprise a travaillé de concert avec les autorités pour obtenir une ordonnance de recherche civile ex parte afin de perquisitionner son domicile. Soupçonnant que des éléments de preuve essentiels seraient stockés sur des ordinateurs à l'endroit en question, l'entreprise a fait appel aux enquêteurs agréés des services judiciaires de Ricoh pour qu'ils se joignent à l'équipe de recherche.

À titre du premier laboratoire judiciaire informatique privé accrédité par l'organisme American Society of Crime Laboratory Directors/Laboratory Accreditation Board, l'équipe des services judiciaires de Ricoh est composée d'un éventail d'experts judiciaires et d'enquêteurs privés agréés réunissant plus de 60 ans d'expérience. Il offre aux conseils d'entreprises et aux cabinets d'avocats une vaste gamme de ressources d'identification, de collecte, de vérification, d'enregistrement et d'analyse de données stockées sous forme électronique (ESI).

SOLUTION

Un expert des services judiciaires de Ricoh s'est donc joint aux policiers et aux enquêteurs privés du client pour mener une perquisition de la demeure du suspect. Un ordinateur a rapidement été repéré au cours de la fouille. L'expert de Ricoh a obtenu une copie-image des données stockées sur l'ordinateur et il a tout de suite entamé une analyse pendant que la fouille se poursuivait dans le reste du domicile.

DÉFI

- Trouver des preuves essentielles liées au piratage de logiciel lors de la perquisition du domicile d'un suspect

SOLUTION

- Analyse judiciaire approfondie de l'ordinateur du suspect afin de repérer le dispositif USB contenant des preuves irréfutables de transactions concernant les produits contrefaits

RÉSULTATS

- Recouvrement de plus de 30 millions de dollars en revenus perdus

Étude de cas

RICOH
imagine. change.
imaginer. changer.

L'analyse a révélé de l'historique Internet contenant des preuves d'opérations bancaires en ligne à partir d'un compte en provenance d'un pays reconnu pour les activités de blanchiment d'argent et la corruption de son système bancaire. L'expert a également récupéré des courriels supprimés qui rendaient compte de correspondances avec un courtier immobilier espagnol concernant l'acquisition d'une propriété d'une valeur de trois millions de dollars située dans un centre de villégiature exclusif en Espagne.

En outre, l'analyse a montré de l'activité impliquant le transfert de données vers un dispositif de stockage USB. Toutefois, les codes enregistrés par le système d'exploitation relatifs au dispositif ne correspondaient aucunement à ceux employés avec les principaux lecteurs USB.

L'expert a donc effectué une recherche sur Internet à partir de son ordinateur portable afin de retracer la source du code : une marque de montre dotée de mémoire USB. Lorsqu'il a montré une image de la montre à l'équipe de recherche, un des membres a affirmé qu'il l'avait aperçue dans la cuisine. La montre a été repérée et l'expert de Ricoh a obtenu une copie-image du dispositif. Une analyse de la copie-image a révélé qu'elle contenait un tableur protégé par mot de passe. Bien qu'il fût persuadé que le cryptage pouvait être décodé au laboratoire de Ricoh, l'expert n'avait pas avec lui les outils nécessaires pour le faire sur place.

Mais il ne s'est pas arrêté là : l'expert de Ricoh a écrit un script pour automatiser la récupération de plus d'un million de mots contenus dans la copie-image de l'ordinateur qu'il avait obtenu tout à l'heure. Tous ces mots ont ensuite été dédoublés et mis à l'essai avec le tableur crypté afin de déterminer si l'un d'entre eux était le mot passe. Après quelque vingt minutes de traitement, le script a identifié le mot de passe pour ouvrir le fichier. Les techniques de criminalistique de pointe employées par l'expert de Ricoh ont permis de découvrir le document qui s'est avéré être la preuve irréfutable du piratage informatique que l'équipe d'enquête espérait trouver.

Le tableur renfermait une liste d'actifs, notamment des comptes bancaires avec leurs soldes et leurs mots de passe. Il contenait également de l'information à propos de transactions liées à la vente des CD contrefaits, dont l'identité des acheteurs, ainsi que d'autres renseignements concernant l'acquisition de la propriété en Espagne.

Durant toutes les étapes de son enquête, l'expert de Ricoh s'est assuré de suivre la procédure juridique par rapport aux copie-images et à la préservation des données en se servant d'outils conformes aux normes de l'industrie.

RÉSULTATS

Grâce aux données récupérées lors de la perquisition, le fabricant de logiciels a pu affirmer que les acheteurs des CD devaient savoir que le logiciel était contrefait, car il était vendu à un tiers du prix régulier. En menaçant d'intenter des poursuites en justice contre ces acheteurs, l'entreprise a réussi à recouvrer de chacun d'eux l'équivalent du prix de détail pour la licence. Elle a ainsi pu récupérer plus de 17 millions de dollars. Plus encore, l'accord de règlement avec l'accusé a permis de récupérer des millions de dollars provenant des comptes bancaires découverts par l'expert de Ricoh.

Il va de soi que le fabricant de logiciels était extrêmement satisfait du travail accompli par l'expert des services judiciaires de Ricoh et des résultats obtenus lors de cette enquête d'une journée.

www.ricoh.ca