KPMG GLD & Associés Monaco

Violation de données notables

■ **CYBER** ■ ACTUALITÉS

■ *Newsletter 2024* ■ *N°1*

Le cas du piratage de Toyota : des répercussions pour l'entreprise et les particuliers

Un grand groupe de cybercriminels, Medusa, a revendiqué le mois dernier la compromission de Toyota Financial Services (TFS) en Allemagne, en obtenant un accès non autorisé à certains de ses systèmes. Le 5 décembre, TFS annonce officiellement sur leur site qu'ils ont été victime de piratage.

Les détails de l'exploitation n'ont pas encore été révélés mais un chercheur en sécurité informatique du nom de Kevin Beaumont a montré qu'en Allemagne, TFS avait une passerelle Citrix exposée à Internet.

Le groupe d'attaquants aurait donc pu exploiter la CVE 2023-4966 nommée « CitrixBleed », exploitée activement depuis l'été Cette même vulnérabilité aurait été exploitée par un autre groupe, LockBit, afin d'obtenir un accès à des systèmes d'informations d'organisations gouvernementales ou encore d'établissements bancaires.

Medusa exigeait un paiement de 8 millions de dollars pour supprimer l'intégralité des données volées. Suivant les recommandations générales concernant la gestion des demandes de rançon et afin de ne pas alimenter ce commerce malveillant, Toyota n'a pas cédé au chantage exercé par le groupe cybercriminel.

© 2024 KPMG GLD et Associés S.A.M., une société anonyme monégasque d'expertise comptable et membre du réseau global KPMG constitué de cabinets indépendants adhérents de KPMG International Limited ("KPMG International"), une société privée à responsabilité limitée par garanties de droit anglais. Tous droits réservés.

En effet, payer la rançon n'assurera ni la suppression des données, ni que l'entreprise ne soit pas à nouveau prise pour cibles par ces attaquants. De plus, en fonction des données qui ont été volée, les pirates peuvent toujours utiliser ces données pour cibler directement les clients (attaques de types phishing et/ou usurpation d'identité) ou revendre leurs données sans que l'entreprise n'en soit informée. L'essentiel est donc de ralentir l'activité de ces cybercriminels.

Comme habituellement dans ce genre de cas, toutes les données volées ont donc été publiées sur le blog des attaquants accessible via le « Dark Web ». Le média allemand Heise a réussi à obtenir le communiqué diffusé par Toyota auprès de ses clients outre-Rhin. Le constructeur les informe que les données fuitées comprenaient des copies de pièces d'identité avec des noms et des adresses, des identifiants et mots de passe de comptes clients ou encore des IBAN client.

Quels enseignements tirer de cet évènement majeur ?

Tout d'abord pour les entreprises, grandes ou petites ; une attention particulière doit être apportée à la sécurité des systèmes exposés à Internet et notamment à leur niveau de sécurité, et pas juste leur état de marche. Les répercussions en termes d'images, et même concernant l'impact sur la vie des clients, mérite de contacter des professionnels de la sécurité informatique.

Enfin, pour les particuliers, il s'agit d'être particulièrement attentif et de se méfier de tout email potentiellement frauduleux et tout appel sans confirmation de la personne au bout du fil. De façon générale, communiquer le minimum d'informations est une façon de se protéger et de protéger sa vie privée.

Sources

- → Toyota alerte ses clients : les pirates de Medusa ont volé des données extrêmement sensibles (tomsguide.fr)
- → https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes
- → https://cybernews.com/news/toyota-financial-services-ransom-attack-exposes-personal-banking-info/
- → https://www.securityweek.com/citrixbleed-vulnerability-exploitation-suspected-in-toyota-ransomware-attack/
- → https://nvd.nist.gov/vuln/detail/CVE-2023-4966

© KPMG GLD et Associés S.A.M., une société anonyme monégasque d'expertise comptable et membre du réseau global KPMG constitué de cabinets indépendants adhérents de KPMG International Limited ("KPMG International"), une société privée à responsabilité limitée par garanties de droit anglais. Tous droits réservés.

Auteurs

Sabina DEBUSSY

Directeur Associé • Advisory • KPMG Monaco

sdebussy@kpmg.mc

Clément MAILLIOUX

Senior Manager • Advisory • KPMG Monaco

cmaillioux@kpmg.mc

© KPMG GLD et Associés S.A.M., une société anonyme monégasque d'expertise comptable et membre du réseau global KPMG constitué de cabinets indépendants adhérents de KPMG International Limited ("KPMG International"), une société privée à responsabilité limitée par garanties de droit anglais. Tous droits réservés.

KPMG GLD et Associés S.A.M renforce son équipe avec une équipe locale dédiée à la Cybersécurité.

Nous accompagnons des entreprises de toutes tailles dans l'évaluation ou l'amélioration de leur sécurité.

- → Audits organisationnels et techniques, tests d'intrusion
- → Assistance pour les plans de continuité d'activité
- → Accompagnement pour la gouvernance de la fonction sécurité
- → Accompagnement pour la Gestion de crise cyber
- → Conseil en durcissement de configuration, architecture sécurisée

Contact

Clément MAILLOUX
Senior Manager IT Risk Advisory / Cyber
cmaillioux@kpmg.mc - +377 97 77 77 17

© KPMG GLD et Associés S.A.M., une société anonyme monégasque d'expertise comptable et membre du réseau global KPMG constitué de cabinets indépendants adhérents de KPMG International Limited ("KPMG International"), une société privée à responsabilité limitée par garanties de droit anglais. Tous droits réservés.

Contactez-nous

Bettina RAGAZZONI
Associée
bragazzoni@kpmg.mc

Stéphane GARINO
Senior Partner
sgarino@kpmg.mc

Xavier CARPINELLI
Associé
xaviercarpinelli@kpmg.mc

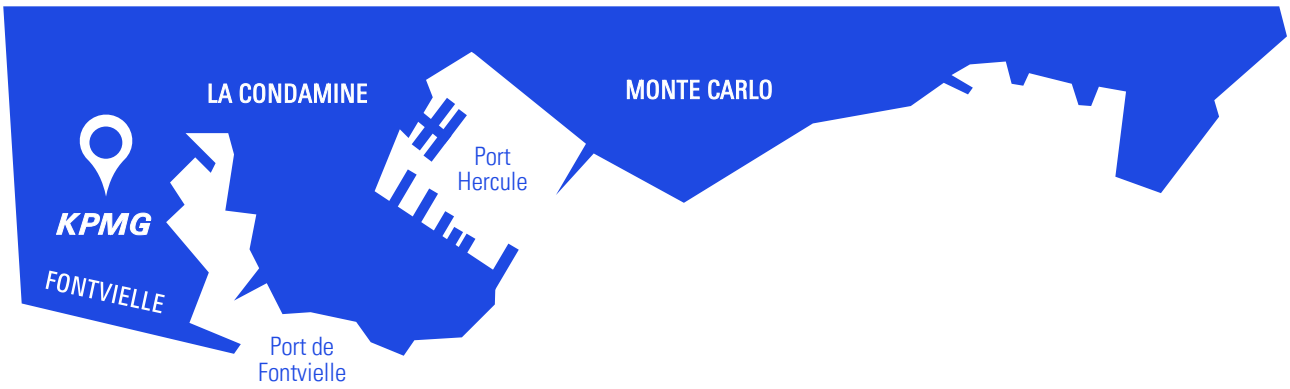
Anne-Marie FELDEN
Directeur Associé
afelden@kpmg.mc

Sylvie ROTI
Directeur Associé
sroti@kpmg.mc

Sabina DEBUSSY
Directeur Associé
sdebussy@kpmg.mc

Bernard SQUECCO
Associé
bsquecco@kpmg.mc

2, rue de la Lüjerneta • "Athos Palace" • 98000, Monaco



mc-news@kpmg.mc
www.KPMG.mc
@KPMG_Monaco
+377 977 777 00
@kpmg-monaco
@KPMGMonaco

Les informations contenues dans ce document sont d'ordre général et ne sont pas destinées à traiter les particularités d'une personne ou d'une entité. Bien que nous fassions tout notre possible pour fournir des informations exactes et appropriées, nous ne pouvons garantir que ces informations seront toujours exactes à une date ultérieure. Elles ne peuvent ni ne doivent servir de support à des décisions sans validation par les professionnels ad hoc. KPMG International ne propose pas de services aux clients. Aucun cabinet membre n'a le droit d'engager KPMG International ou les autres cabinets membres vis-à-vis des tiers. KPMG International n'a le droit d'engager aucun cabinet membre.

© KPMG GLD et Associés S.A.M., une société anonyme monégasque d'expertise comptable et membre du réseau global KPMG constitué de cabinets indépendants adhérents de KPMG International Limited ("KPMG International"), une société privée à responsabilité limitée par garanties de droit anglais. Tous droits réservés.