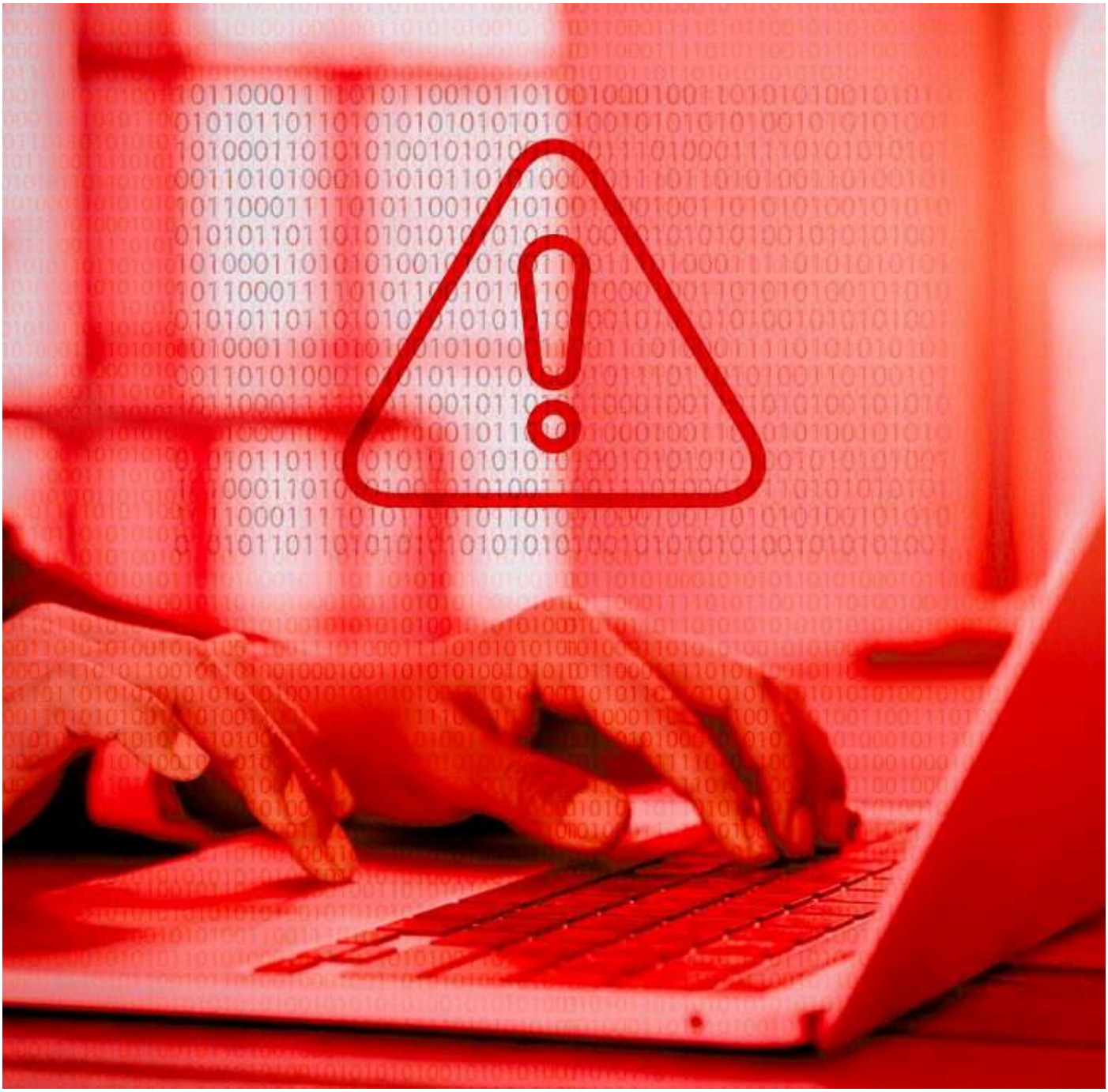
[CYBERATTAQUE]

Cybersecurite

Direct Assurance victime d'une fuite de données, RIB et IBAN dans la nature

22 novembre 2024



A chaque jour sa nouvelle attaque et le groupe cybercriminel near2tlg semble être hyperactif. Après Le Point, SFR et Mediboard, les hackers ont visé la filiale d'Axa en courtage d'assurances.

near2tlg a encore frappé. Le groupe de hackers, qui s'est déjà illustré en frappant Le Point, SFR ou encore le logiciel de santé Médiboard, récidive en attaquant Direct Assurance. Le « N°1 de l'Assurance en ligne », qui n'a pas encore réagi officiellement, aurait ainsi été victime d'une violation de données.

Ce sont quelques 6000 clients et 9000 prospects dont les informations ont été dérobées par les cybercriminels. Noms, prénoms, adresses mail et numéros de téléphone ont fuités et, plus grave, pour 5600 d'entre eux, les RIB et IBAN sont aussi dans les mains des pirates.

La compromission date du 14 novembre, « *avec un accès employé* » assure le groupe. Selon nos informations, le groupe cybercriminel aurait procédé en s'en prenant à un prestataire de Direct Assurance. On notera que les hackers ont déclaré sur un forum tristement célèbre avoir prévenu au préalable les entreprises victimes de l'existence de « *failles de sécurité* » dans leurs systèmes.

Lire aussi...

➜ **Message Signing de Retarus garantit l'authenticité et la sécurité des e-mails**

➜ **Projet de loi - Création du Centre de développement des capacités cyber dans les Balkans occidentaux**

➜ **Les MSP peuvent dorénavant proposer la plateforme de Mimecast à leurs clients**

L'article de la semaine

➜ **Comment l'IA générative bouleverse les codes de la gestion documentaire ?**

Guillaume Perissat

À LIRE ÉGALEMENT :

Sysdig nomme un nouveau CEO
22 novembre 2024

AVIS D'EXPERT - Comment l'IA contribue à rendre les réseaux plus sûrs
22 novembre 2024

Cybermenaces : "Il est nécessaire d'accélérer les processus réglementaires", Myriam Quéméner,experte auprès du Conseil de l'Europe
22 novembre 2024

Service

- Actualités
- Dossiers
- Magazine
- Livres Blancs
- Web Conférences
- Télétravail
- Équipement matériel
- Annuaire sécurité
- Partenaires

Informations

- Identification
- Inscription
- RSS
- Plan du site
- Mentions légales
- Charte de confidentialité
- CGV

Contactez-nous par mail

Abonnez-vous à notre Newsletter

[CYBERATTAQUE]

Cybersecurite

Les cybercriminels de near2tlg rançonnent les données de santé de 750 000 français

22 novembre 2024

Le groupe cybercriminel a infiltré le logiciel Mediboard, très utilisé dans le milieu de la santé, pour mettre la main sur les données de centaines de milliers de patients.

Le 19 novembre, le groupe cybercriminel near2tlg a dérobé les données de 750 000 patients d'établissements de santé français. Les hackers ont pu s'emparer de ses informations en ciblant Mediboard, une application open source utilisée par les hôpitaux et cabinets médicaux pour gérer et transférer les dossiers de patients et organiser les rendez-vous.

Le groupe cybercriminel revendique également des attaques directes contre des hôpitaux en France et au Luxembourg, et s'en est au passage pris à Direct Assurance. L'éditeur de Mediboard, Xtrem Santé, filiale de Softway Medical, a déclaré qu'un de ses clients a été victime d'une usurpation d'un compte avec accès à privilèges.

Lire aussi...

➜ **Message Signing de Retarus garantit l'authenticité et la sécurité des e-mails**

➜ **Projet de loi - Création du Centre de développement des capacités cyber dans les Balkans occidentaux**

➜ **Les MSP peuvent dorénavant proposer la plateforme de Mimecast à leurs clients**

L'article de la semaine

➜ **Comment l'IA générative bouleverse les codes de la gestion documentaire ?**

Fuite de données sensibles

Les pirates ont publié des échantillons de données. Lesquelles incluent nom, le prénom, la date de naissance, l'adresse et le numéro de téléphone du patient, mais aussi des informations de santé à l'instar du médecin traitant, des antécédents médicaux, des prescriptions ou encore des déclarations de décès. Les données en question n'ont pas encore été mises à la vente, near2tlg menaçant de les divulguer si une rançon de 5000 dollars ne lui est pas versée.

Pour Matthieu Trivier, Directeur avant-vente EMEA chez Semperis, « *bien que les informations soient encore limitées, les premiers rapports suggèrent que plusieurs établissements ont été touchés, impactant potentiellement jusqu'à 2 millions de patients* ». Il poursuit : « *ces comptes utilisateurs, qui ouvrent l'accès aux données et services les plus sensibles, constituent des cibles de choix pour les cybercriminels, et une gestion approximative des droits d'accès peut rapidement créer des brèches significatives, fragilisant l'ensemble du système* ».

Guillaume Perissat

À LIRE ÉGALEMENT :

Sysdig nomme un nouveau CEO
22 novembre 2024

AVIS D'EXPERT - Comment l'IA contribue à rendre les réseaux

Cybermenaces : "Il est nécessaire d'accélérer les processus réglementaires",

plus sûrs
22 novembre 2024

Myriam Quéméner,experte auprès du Conseil de l'Europe
22 novembre 2024