communiqué de presse

econocom

24 août 2023

Information cybersécurité : mise à jour de la communication du 23 août 2023 Jeudi 24 août 2023, 17h00

Le groupe Econocom confirme une attaque de cybersécurité qui fait l'objet d'une investigation sérieuse et de mesures d'endiguement. Les dernières investigations montrent que les informations fuitées proviendraient d'un prestataire intervenant pour quelques clients Econocom en France. Aucun système ou base de données internes à Econocom ne seraient affectés, et l'analyse des données exfiltrées ne permet pas à ce jour d'identifier la divulgation de données sensibles.

Dimanche 20 août, un groupe d'attaquants a revendiqué via un post Twitter avoir piraté Econocom, et a commencé à publier des données. Aucune demande de rançon n'a été reçue par le groupe. Un dépôt de plainte est en cours.

Dès prise de connaissance de cet incident, l'équipe Group Security et le Security Operations Center d'Econocom se sont immédiatement mobilisés, et ont lancé les premières investigations. Celles-ci ne permettant pas de détecter d'actions malveillantes au sein du SI d'Econocom, l'hypothèse la plus plausible était qu'il s'agissait d'une réminiscence d'une précédente attaque en 2020 (documents diffusés très anciens), aujourd'hui circonscrite, dont Econocom avait été victime.

Le mardi 22 août aux alentours de 15h, Econocom constate que des données plus récentes ont été exfiltrées et active le dispositif de gestion de crise cyber : les données exfiltrées sont trouvées sur deux partages SharePoint à usage individuel (créés via Teams). Ces dossiers comportent peu de données, et ont été isolés dès leur identification mardi 22 août 2023, respectivement à 16h00 et 18h00. Tous les accès à ces SharePoints ont ainsi été bloqués. L'infrastructure SharePoint d'Econocom prévient en outre toute forme de propagation vers d'autres systèmes. Par ailleurs, l'analyse des données exfiltrées ne permet pas à ce jour d'identifier de données sensibles.

Le mercredi 23 août matin, les investigations montrent qu'un poste utilisateur d'un prestataire d'Econocom en France serait à l'origine de la fuite de données. Le prestataire a immédiatement été contacté pour, en collaboration avec ses équipes, identifier puis bloquer la source de l'attaque et analyser ses impacts exhaustifs. Le personnel de ce prestataire, qui se connecte à une ressource Econocom par VPN pour récupérer les documents nécessaires à l'exécution de ses missions, est identifié et les accès des postes aux ressources Econocom sont révoqués. Les investigations confirment que les données fuitées sont issues d'un espace de partage chez le fournisseur.

A ce jour, la piste la plus plausible est ainsi que le prestataire a été compromis et que les données ont été exfiltrées depuis ses infrastructures. Toutefois, les investigations et mesures de confinement se poursuivent chez Econocom pour s'assurer qu'aucun système interne n'a été compromis.

Toute nouvelle évolution significative sera communiquée en toute transparence aux parties prenantes du groupe, y compris aux autorités compétentes.

POUR PLUS D'INFORMATIONS

www.econocom.com
Suivez-nous sur LinkedIn et Twitter
Contact presse agence :
econocom@the-arcane.com
Contact presse Econocom :
olivier.beaunay@econocom.com