LEMAGIT

URL :http://www.lemagit.fr/
PAYS :France
TYPE :Web Grand Public

► 28 août 2023 - 11:03

> Version en ligne

Cyberattaque : Econocom ferme un point d'entrée sur son système d'information

lemagit.fr/actualites/366549472/Stormous-et-GhostSec-tentent-de-faire-chanter-Econocom

Valéry Rieß-Marchive

par

Valéry Rieß-Marchive, Rédacteur en chef

Publié le: 28 août 2023

[Mise à jour, le 28 août 2023 @ 13h45] Econocom a publié, ce lundi matin, un nouveau communiqué de presse expliquant que ses investigations « confirment que les informations fuitées proviennent d'un prestataire intervenant pour quelques clients d'Econocom en France ».

Selon l'ESN, « dans leur immense majorité, ces données sont peu sensibles, à l'exception de données privées d'une seule personne ainsi que des données de connexion de comptes techniques, hébergées chez le prestataire ». Dès lors, les équipes d'Econocom travaillent « avec les clients concernés et identifiés pour limiter au maximum les impacts potentiels ».

Les marqueurs techniques collectés dans le cadre des investigations ont été utilisés pour « mener des vérifications sur le système d'information interne Econocom ». Celles-ci ont fait apparaître, « vendredi 25 août au soir, la trace d'une attaque identique à celle subie par notre prestataire ».

Dans son communiqué, l'ESN précise qu'il s'agit d'un seul serveur, « au contenu peu sensible », qui a pu être « immédiatement cantonné ». En outre, « les investigations menées pendant la nuit du vendredi au samedi ont démontré que les mesures de sécurité en place ont permis d'empêcher toute fuite d'information ou compromission par cette voie ».

Toujours très prudent dans ses déclarations alors que les investigations se poursuivent, Econocom indique toutefois qu'au regard « de l'ensemble des analyses conduites et des éléments » disponibles à date, « aucun système ou donnée interne Econocom n'aurait été compromis par cette seconde attaque ».

L'ESN s'engage à « continuer de communiquer régulièrement sur cet incident jusqu'à sa résolution totale ».

[Mise à jour, le 24 août 2023 @ 17h30] Dans un nouveau communiqué de presse, Econocom explique que « dès la 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 n'ont pas conduit à la détection

d'actions malveillantes au sein du système d'information d'ESN. Dès lors, l'hypothèse privilégiée initialement était celle d'un recyclage des données volées par Pysa lors de la cyberattaque de 2020.

Las, explique François-Xavier Vincent, responsable de l'équipe Group Security d'Econocom, dans un échange téléphonique avec la rédaction, « le mardi 22 août dans le milieu de l'après-midi, Econocom constate que des données plus récentes ont été exfiltrées et active le dispositif de gestion de crise cyber ».

Les données exfiltrées sont alors rapidement « trouvées sur deux partages SharePoint à usage individuel (créés via Teams) ». Ils comportent peu de données, et « ont été isolés dès leur identification mardi 22 août 2023, respectivement à 16h00 et 18h00 ».

Les accès à ces partages ont été bloqués et l'infrastructure « SharePoint d'Econocom prévient toute forme de propagation vers d'autres systèmes ». En outre, « l'analyse des données exfiltrées ne permet pas à ce jour d'identifier de données sensibles », précise le communiqué de l'ESN.

Ce mercredi 23 août au matin, les investigations permettent de remonter jusqu'au poste utilisateur d'un prestataire d'Econocom : « 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 », indique l'ESN. Et de préciser que « 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 ».

À ce stade, cette piste apparaît donc comme « la plus plausible ». Malgré cela, « les investigations et mesures de confinement se poursuivent chez Econocom pour s'assurer qu'aucun système interne n'a été compromis ». Il s'agit encore, notamment, d'établir comment le poste utilisateur du prestataire a été initialement compromis.

[Article original, le 23 août 2023 @ 13h56] Ce samedi 19 août, GhostSec et Stormous revendiquent un vol de données sur le système d'information d'Econocom. Plus de 70 giga-octets de données seraient concernés, selon le premier groupe de cyberdélinquants, partenaire du second pour la diffusion des fichiers.

À première vue, les données divulguées peuvent donner l'impression d'un recyclage de celles volées à Econocom à l'automne 2020, par Pysa, et publiées sur un site accessible via Tor, au début du mois de janvier suivant. Mais certains fichiers présentent une date de création trop récente pour cela, laissant à suspecter une nouvelle intrusion, plus récente.

Sollicité ce lundi 21 août sur cette question par la rédaction, ni le service de presse d'Econocom, ni la personne chargée des relations investisseurs n'a répondu à notre e-mail, à l'heure où ces lignes sont publiées. **[Note à 15h20 : un porte-parole de l'ESN précise avoir cherché, en vain, à joindre la rédaction par téléphone, ce mardi 22 août. Aucun message n'a toutefois été laissé]**

Joint par e-mail en début de semaine, le groupe Stormous, sorti d'une certaine torpeur plus tôt cette année, a assuré n'avoir aucun lien avec Pysa. Surtout, GhostSec a assuré à la rédaction qu'il s'agissait bien d'une nouvelle cyberattaque : « il s'agit d'une nouvelle brèche, les fichiers sont anciens et nous publierons bientôt de nouveaux échantillons. Nous sommes en train d'organiser davantage de données et d'informations à leur encontre ». Et de revendiquer avoir eu « un accès total », « une semaine avant » la revendication. Mais sans préciser ce à quoi le groupe avait eu accès.

Depuis, de nouveaux fichiers et dossiers ont effectivement commencé à être divulgués sur le site vitrine de Stormous – accessible de manière pour le moins erratique.

Il aura fallu attendre ce mercredi 23 août pour que l'entreprise de services numériques (ESN) réagisse publiquement, en publiant un communiqué sur son site Web. Dans celui-ci, Econocom « annonce une alerte de cybersécurité sans impact significatif à ce stade ». Et d'indiquer que « les investigations en cours montrent que la compromission se limite à un dossier partagé. Aucune fuite d'informations sensibles n'a été identifiée à ce jour ».

L'ESN assure en outre faire « tout son possible pour limiter l'ampleur du problème, contenir la fuite de données et en limiter l'impact ».