Comment **Sopra Steria** a déjoué l'attaque du rançongiciel Ryuk ?

« Les cordonniers sont les plus mal chaussés ». Ce proverbe a été largement utilisé pour dépeindre la cyberattaque dont a été victime Sopra Steria. Mais l'ESN a pourtant bloqué l'attaque avant qu'elle ne se propage sur son SI, et surtout auprès de ses clients, dans une gestion jugée exemplaire par l'Anssi. Récit d'une attaque avortée qui n'est cependant pas sans conséquences pour la deuxième ESN de France.

« Perdre 40 à 50 millions d'euros pour une attaque qui a échoué donne une idée de l'impact qu'aurait eu une attaque réussie »

Jean-Claude Laroche, vice-président du Cigref et DSI du groupe Enedis.

« *Il y a des cibles qui savent réagir [...] Sopra Steria : c'est certes une attaque, mais ce n'est pas une attaque réussie* », soulignait Guillaume Poupard, directeur général de l'Anssi, le 4 novembre dernier lors d'une audition au Sénat. Pour l'agence nationale de la sécurité des systèmes d'information, l'ESN fait partie des exemples à suivre dans la gestion d'une cyberattaque par ransomware. Un phénomène qui a explosé en 2020. « *Nous avons traité 54 attaques par rançongiciel en 2019. Au 30 septembre 2020, ce nombre était de 128 ! C'est donc un phénomène particulièrement inquiétant. Et il n'y a pas de raisons que cela s'infléchisse à court terme [...] Les attaques sont de plus en plus ciblées et les rançons se chiffrent désormais en millions, voire en dizaines de millions [d'euros]* », a précisé le patron de l'Anssi. Dans ce contexte, les « bons élèves » sont donc à saluer. Et c'est le cas de Sopra Steria, estime l'agence nationale.

Comment l'ESN a déjoué l'attaque ? « *Ils l'ont détecté très tôt et ont été capables de la bloquer. En fait, elle n'a touché, peut-être, que quelques dizaines d'ordinateurs. Ils ont été extrêmement prudents en éteignant intégralement de grands systèmes pour ne pas contaminer leurs clients* », a résumé Guillaume Poupard. Selon lui : « *Sopra Steria a su réagir vite et mettre en place une organisation de gestion de crise pour traiter l'incident* ». Au final, il s'agit donc d'une « *attaque qui a été déjouée par un acteur suffisamment mature* ».

Cette « maturité », mise en exergue par l'Anssi, n'est pas réellement surprenante puisque Sopra Steria possède elle-même une activité de cybersécurité, principalement via sa filiale I2S. Cette entité propose notamment des services de SOC (Security Operations Center), qualifiés par l'Anssi pour répondre aux exigences de sécurité des Opérateurs d'Importance Vitale (OIV). La liste exacte de clients d'I2S n'est pas publique. Mais elle compte des services de l'État et des grands groupes. C'est grâce à ses compétences en matière de cybersécurité, que Sopra Steria a réussi à déjouer l'attaque, estime l'Anssi. Pour autant, son SI n'était pas infaillible et il aura fallu cinq jours avant que l'intrusion ne soit repérée.

Une version inconnue de Ryuk

La chronologie de l'attaque débute autour du 15 octobre. Selon plusieurs sources, les assaillants ont exploité le botnet Trickbot pour s'introduire sur le SI de Sopra Steria. Découvert en 2016, ce malware est en général utilisé pour préparer le terrain de Ryuk, un rançongiciel qui a particulièrement le vent en poupe auprès des cybercriminels. Depuis 2018, Ruyk a été exploité dans le cadre de plusieurs campagnes d'attaques, dont la plus importante a pris pour cible la chaîne d'hôpitaux américaine Universal Health Services (UHS), en septembre 2020. Selon un classement du FBI, paru en mars dernier, Ryuk est aujourd'hui le ransomware le plus lucratif pour les cybercriminels avec 61 millions de dollars rançonnés entre février 2018 et octobre 2019.

C'est le 20 octobre au soir, que les équipes informatiques de Sopra Steria repèrent l'attaque. Elle est bien basée sur le rançongiciel Ryuk, mais dans une nouvelle variante. « *Le virus a été identifié : il s'agit d'une version du ransomware Ryuk jusque-là inconnue des éditeurs d'antivirus et des agences de sécurité* », indiquera l'ESN dans une publication postée sur son site le 26 octobre. « *Les équipes d'investigation de Sopra Steria ont immédiatement fourni toutes les informations nécessaires aux autorités compétentes. La signature de cette nouvelle version du virus a donc pu être rapidement communiquée à tous les éditeurs d'antivirus pour mise à jour de leurs antivirus* ».

En interne, les collaborateurs sont informés par email dès le 21 octobre que le groupe « *fait l'objet d'une attaque depuis la veille* ». Dans la foulée, Sopra Steria communique aussi auprès du grand public. Sans alors préciser qu'il s'agit de Ryuk, une information de quelques lignes est publiée sur son site internet le 21 octobre. Elle indique simplement qu'une « *cyberattaque a été détectée sur le réseau informatique le 20 octobre au soir* » et que « *des mesures de sécurité ont été prises afin de limiter les risques de propagation* ». Ce n'est que le 26 octobre que cette information est « actualisée » et que l'identité du ransomware est divulguée auprès du grand public.

Dès le 21 octobre, Sopra Steria communique également auprès de ses clients, en partageant cette fois tous les détails dont elle dispose, y compris l'identité du rançongiciel. « *Sopra Steria s'est démarquée par sa transparence auprès de ses clients qui ont été immédiatement informés de l'attaque. C'est d'ailleurs la première fois qu'un acteur fait autant preuve de transparence auprès de ses clients* », souligne Jean-Claude Laroche, vice-président du Cigref et DSI du groupe Enedis, justement un des grands clients de l'ESN. « *Nous avons alors isolé nos systèmes du SI de Sopra Steria et travaillé avec leurs équipes sur la gestion de crise et la remédiation* ».

Plus de 10 jours de shutdown

Comme l'a évoqué Guillaume Poupard, la première mesure technique prise par les équipes informatiques de Sopra Steria fut d'arrêter tous les systèmes et services pour éviter la propagation de l'attaque en interne et surtout pour protéger ses clients. Rappelons que l'ESN compte comme clients des opérateurs d'importance vitale, plusieurs ministères dont celui de la Défense, ainsi que des grands groupes tels que La Poste, Airbus ou Enedis. « *Protéger sa clientèle a clairement été une priorité de Sopra Steria. Dans ce type d'attaques, ciblant des acteurs IT, les clients et partenaires peuvent aussi être des cibles potentielles, par rebond* », souligne Nicolas Caproni, responsable de l'équipe Cyber Threat Intelligence chez Sekoia, deeptech française spécialiste de l'anticipation des menaces cyber. Dans ce contexte, l'ESN a pris la mesure la plus drastique possible avec une coupure complète du SI pour éviter tout risque de propagation. Même si Ryuk cible les machines Windows, Sopra Steria a fermé également ses systèmes tournant sur Linux ou Solaris. « *Nous n'avions plus accès aux applications métiers, ni même à la messagerie. Tout était bloqué* », explique-t-on de source interne. Sopra Steria compte près de 46 000 collaborateurs répartis dans 25 pays, qui se sont donc retrouvés privés de leurs principaux outils de travail. Les managers ont alors encouragé leurs collaborateurs à poser des congés ou des RTT. Les prestataires en mission chez des clients pouvaient bien entendu continuer d'utiliser des outils non connectés au SI de Sopra Steria. Mais selon nos informations, certains clients ont suspendu les missions des prestataires de l'ESN et même bloqué leur accès physique aux sites par mesure de précaution. « *L'attaque est tombée juste au moment de l'élaboration du rapport d'activité mensuel, qui sert à la réévaluation des salaires et à la déclaration des heures supplémentaires. Comme il a été impossible de le terminer. Les salaires ont été versés sur les mêmes montants, avec une régularisation qui se fera prochainement* », indique une source syndicale.

Le shutdown du SI a débuté autour du 21 octobre, avec une réouverture progressive à compter de la première semaine de novembre. Plus précisément, une grande de partie du SI a été remise en service le 6 novembre, dont les infrastructures centrales du groupe, les serveurs d'applications ainsi que les « *environnements R&D et de projets clients* », indique une source proche du dossier.

L'attaque a donc entraîné plus d'une dizaine de jours de blocage du SI. Côté client, des mesures ont cependant été mises en place pour préserver un minimum d'activité. « *Nous avons déployé certaines mesures de contournement pour pouvoir travailler en mode dégradé, avec notamment des postes de travail à nous. Mais il y a eu clairement une rupture d'activité équivalente à une semaine de travail, étalée sur deux à trois semaines* », poursuit Jean-Claude Laroche.

Le plan de remédiation et de reprise d'activités a été élaboré le 22 octobre et mis en place dès le 26. Il intégrait notamment un


sopra steria

Vos enjeux Services Secteurs d'activité Perspectives Car

Accueil / Médias / Communiqués / Communiqué

Information sur une cyberattaque

21 octobre 2020

Une cyberattaque a été détectée sur le réseau informatique de Sopra Steria le 20 octobre au soir.

Des mesures de sécurité ont été prises afin de limiter les risques de propagation.

Les équipes du Groupe sont pleinement mobilisées pour assurer un retour à la normale le plus rapidement possible et tout est mis en oeuvre pour assurer la continuité de l'activité.

Sopra Steria est en contact étroit avec ses clients et partenaires ainsi qu'avec les autorités compétentes.

Lire la suite dans L'1FO-CR n°2