No More Ransom a tiré 2500 victimes des griffes des ransomwares

La contre-offensive anti-ransomwares marque des points. Notamment grâce au projet No More Ransom, qui développe et met à disposition des outils de déchiffrement. Ces outils ont aidé plus de 2□500 victimes à récupérer leurs données, annonce Kaspersky, membre de l'initiative de lutte contre les rançongiciels créée le 25 juillet dernier aux côtés d'Intel Security (ex-McAfee entre temps revendu à TPG) en association de la police néerlandaise (National High Tech Crime Unit) et Europol (European Cybercrime Centre).

No More Ransom propose aujourd'hui 7 outils de déchiffrement propres à certaines familles de malwares cryptographiques dont WildFire, Teslacrypt, CoinVault ou Chimera. Rappelons que la plupart du temps, si un ransomware est activé, il lance le chiffrement des fichiers ciblés par ses concepteurs, en local (disque dur de la machine) ou, pire, en réseau. En l'absence de sauvegarde, le seul moyen de retrouver les données est alors de payer la rançon exigée par les cybercriminels afin d'obtenir la clé de déchiffrement. Sans garantie de résultat d'ailleurs. Ou de se tourner vers le projet de lutte contre ce nouveau fléau soutenu par Eurojust et la Commission européenne. Selon Europol, No More Ransom aurait déjà privé les cybercriminels de près de 1,35 million d'euros, en permettant aux victimes de récupérer leurs données sans avoir à payer de rançon.

13 nouveaux pays

Fort de ce succès, No More Ransom va poursuivre son développement. Le projet reçoit aujourd'hui le renfort des agences de 13 nouveaux pays* dont la France. D'autres agences gouvernementales et organisations du secteur privé devraient rejoindre le programme dans les mois qui viennent, promettent ses initiateurs. *« La lutte contre les ransomwares offre de meilleurs résultats quand les agences de protection de la loi et les entreprises privées travaillent main dans la main*, déclare Jornt van der Wiel, chercheur en sécurité au sein de l'équipe de recherche et d'analyse (GReAT) de Kaspersky Lab. *Les chercheurs peuvent offrir une meilleure analyse des malwares et des services d'Internet scanning, pour trouver des liens entre différents morceaux de données. Avec ces informations, la police est à même de localiser et saisir plus facilement les serveurs utilisés pour gérer les attaques. »* Et il arrive parfois que ces serveurs contiennent les clés de déchiffrement. Elles sont alors reversées dans les outils de déchiffrement publiés sur le site du projet anti-ransomware.

No More Ransom va poursuivre son action. D'abord en privilégiant la coordination entre les différents représentants des pays désormais membres du projet. Ensuite en poursuivant le développement d'outils de récupération des fichiers chiffrés. Enfin, en élargissant le nombre de langues supportées par le site web pour l'heure proposé en anglais uniquement. De nouvelles entreprises privées devraient également rejoindre l'initiative, annonce le communiqué sans préciser leur nature ni le rôle qu'elles joueront dans l'organisation. Il est fort probable que ce soit des acteurs de la sécurité. Des plus louables, l'initiative ne manquera pas de travail. Les cybercriminels ne cessent de faire preuve d'imagination pour piéger les victimes potentielles et renforcent les techniques de chiffrement des fichiers. En matière de ransomware, le jeu du

gendarme et du voleur ne fait que commencer.

** France (Police Nationale), Bosnie-Herzégovine, Bulgarie, Colombie, Espagne, Hongrie, Irlande, Italie, Lettonie, Lituanie, Portugal, Royaume-Uni et Suisse.*

Lire également

Ransomware : les entreprises françaises passent à la caisse
Ransomware : un gang engrange 121 millions de dollars en 6 mois
Comment un chercheur français a infecté des arnaqueurs avec Locky