Télégrammes : Locky en vacances, Oracle Cloud s'étend en UK, Hadoop et Couchdb rançonnés, MTI racheté

Locky a pris des vacances pour Noël. C'est un phénomène inattendu auquel les spécialistes de la sécurité ont assisté. Les statistiques sont formelles, le ransomware Locky s'est octroyé une pause pendant les fêtes de fin d'année. Sa diffusion a chuté de 81% entre le 24 décembre et le 3 janvier. La raison de cette chute vient de l'arrêt d'un botnet Necurs aussi vecteur du trojan bancaire Dridex avant de privilégier Locky plus rémunérateur. Dans le même temps, le kit d'exploit Angler a pris également des vacances. Pendant la période des fêtes, la famille Locky avait trouvé refuge sur un autre botnet, Kovter qui diffusait des campagnes de spams. Ce n'est malheureusement pas pour autant la fin de Locky. Les experts s'attendent à ce que Necurs reprenne du service après plusieurs semaines de congés bien payées.

Cloud : Oracle s'étend en Grande-Bretagne. En pleine offensive sur le Cloud public, Oracle annonce l'ouverture de trois nouvelles régions, en Grande-Bretagne, en Turquie et aux Etats-Unis. Les datacenters permettant d'opérer ces services devraient être disponibles à la mi-2017, amenant le Cloud d'Oracle à 29 implantations géographiques (ou régions) au niveau mondial. Chaque nouvelle zone géographique du Cloud de Redwood Shores est composée de 3 datacenters reliés par des liens haut débit et distants de plusieurs kilomètres l'un de l'autre afin de fournir le maximum de garanties en matière de haute disponibilité. Outre-Manche, l'éditeur américain s'implantera à Londres.

Prise d'otage du NoSQL : Hadoop et Couchdb aussi. Après la prise d'otages de multiples instances MongoDB non sécurisées (34 500 à l'heure où nous écrivons ces lignes), puis de bases ElasticSearch (4 600), les cybercriminels s'attaquent aux environnements Hadoop et Couchdb, signalent les deux chercheurs en sécurité qui suivent la progression de ces attaques contre les technologies NoSQL, Victor Gevers et Niall Merrigan. Ce dernier signale ainsi que 115 bases Hadoop ont été victimes d'actes de vandalisme (à priori sans demande de rançon). Tout récemment, plusieurs personnes sur Twitter ont aussi signalé que des bases Couchdb non sécurisées étaient à leur tour l'objet de demandes de rançon. Rappelons que les cybercriminels repèrent des bases librement accessibles sur Internet, en copie les données avant de réclamer une rançon au propriétaire. La technique d'une grande simplicité semble toutefois peu rentable, la plupart des bases exposées renfermant des environnements de développement pour lesquelles les entreprises ne sont pas prêtes à payer.

MTI Europe racheté par Endless. L'intégrateur IT spécialisé dans le stockage était la propriété de fonds Garnett et Helfrich Capital LLP. Il vient d'être racheté par un autre fonds d'investissement, IV d'Endless LLP. Le montant de l'opération n'a pas été dévoilé. MTI est présent en Angleterre, son siège social, mais également en Allemagne et en France. Avec ce changement d'actionnaires, Endless prévoit d'utiliser ses capacités de transformation, de « *buy & build* », en s'appuyant sur son expérience en tant que propriétaire d'entreprises similaires dans le secteur. Son objectif est de soutenir la croissance de l'entreprise au cours des prochaines années.