WannaCry 2.0 : Renault n'est pas la seule entreprise touchée en France

C'est probablement l'un des effets les plus spectaculaires de WannaCry en France. Ce lundi, l'immense parking de l'usine Renault de Douai est presque vide, conséquence de l'infection du constructeur automobile par le 'ransomworm', autrement dit la combinaison d'un ransomware et d'un ver. Selon l'AFP, les 3 500 salariés de l'usine ont été mis au chômage partiel et bénéficieront d'un jour de congé collectif. Une décision prise « *préventivement* », assure un porte-parole du groupe, avec un sens de la litote consommé.

Renault espère sécuriser le site dans la journée *« pour que le travail puisse reprendre demain (mardi) matin »*, explique un responsable de la communication de l'usine à l'AFP. Un travail essentiellement préventif, mais nécessitant une grande vigilance, ajoute-t-il. Autrement dit, les équipes du constructeur cherchent encore à prendre la mesure de l'infection par WannaCry et à redémarrer les systèmes petit à petit. La CGT explique que le parc informatique de l'usine comprend plusieurs centaines d'ordinateurs, qui doivent être mis à jour avant d'être remis en service. Les syndicats font également état de robots qui ont mis hors service afin d'être vérifiés.

Anssi : plusieurs cas en France

La société semble toutefois avoir pu redémarrer ses autres sites touchées par WannaCry juste avant le week-end, notamment l'usine Dacia de Pitesti (Roumanie), celles de Novo Mesto (Slovénie), celle de Batilly (Meurthe-et-Moselle) ou encore celle de Sandouville (Seine-Maritime), des unités dont la production a été arrêtée ce week-end.

Évidemment, et contrairement aux premières affirmations, qui ont circulé, Renault n'est pas la seule entreprise touchée en France, comme l'a confirmé Guillaume Poupard, le patron de l'Anssi (Agence nationale de la sécurité des systèmes d'information) au micro de France Inter ce matin. Ce qui pourrait indiquer d'autres cas sérieux, l'Anssi étant plutôt appelée en pompier sur des incidents majeurs menaçant sérieusement le fonctionnement d'une entreprise.

Attaque massive et simultanée

Chez Wavestone, Gérôme Billois, senior manager en gestion des risques et sécurité, évoque un week-end chargé avec plusieurs interventions auprès de sociétés en France et en Europe que le cabinet accompagne dans leur gestion de crise. De son côté, Airbus Cybersecurity explique avoir communiqué à ses clients des marqueurs caractérisant l'infection dès vendredi soir. Lundi matin, le prestataire expliquait avoir la quasi-certitude qu'un de ses clients était impacté.

Chez Kaspersky, Tanguy de Coatpont, directeur général France et Afrique du Nord, souligne que si certains de ses clients ont bien détecté l'attaque, aucun n'est actuellement en situation de crise. « *Via nos technologies heuristiques, nos solutions ont arrêté l'attaque, tant sur les postes de travail que côté serveurs* », assure le dirigeant, qui souligne toutefois le caractère massif et simultané de l'attaque

(200 000 postes infectés en un week-end, dans de nombreux pays). « *C'est inhabituel par rapport aux autres campagnes de ransomwares qui s'étalent davantage dans le temps* », ajoute-t-il.

Le message est similaire chez Trend Micro, autre éditeur d'outils de protection. Son directeur de la stratégie cyber pour l'Europe du Sud, Loïc Guézo, explique également que WannaCry est détecté par les outils maison, tant en sandboxing que lors de la réplication sur un réseau. « *En réalité, cette affaire souligne des questions de gouvernance de la sécurité des systèmes d'information, comme celle du raccourcissement des cycles d'application des patchs de sécurité ou celle de la protection des systèmes industriels. WannaCry a infecté des systèmes d'affichage de trains, des usines, des distributeurs de billets, des systèmes dans des hôpitaux. On est à une épaisseur de trait de l'accident industriel causé par une cyberattaque…* », prévient-il.

A lire aussi :

WannaCry et maintenant les variantes !

WannaCry : autopsie du ransomware 2.0, boosté par les exploits de la NSA

La parade n'existe pas pour contrer les futures affaires WannaCry