Télégrammes : Une faille Windows à 90 000 dollars; ServiceNow rachète BrightPoint; Sopra Steria monte au capital d'Axway; Premières attaques DDoS TFTP.

- **90 000 dollars pour une faille zero day sur Windows.** Une vulnérabilité accordant une escalade des privilèges sur l'OS de Microsoft a été mise en vente 90 000 dollars sur le site exploit.in, un forum d'échange pour les cybercriminels. Le vendeur, BuggiCorp, fait même la démonstration dans une vidéo de sa faille critique. Elle fonctionne avec la plupart des versions de Windows, de 2000 au dernier millésime Windows 10. C'est l'équipe Spiderlabs de Trustwave qui a détecté cette vente un peu surprenante. Elle considère cette proposition comme valide et le vendeur utilise un système de séquestre où le paiement ne s'effectue que quand l'acheteur est content de son achat.
- **ServiceNow rachète BrightPoint.** Le spécialiste de l'ITSM va se renforcer dans la cybersécurité dans le Cloud avec cette acquisition. BrightPoint a été fondé en 2011 par un ancien RSSI de Merryll Lynch et offre une approche analytique distribuée pour la prévention et la détection en matière de cybersécurité. La start-up avait été connue sous le nom Vorstack avant son changement de nom il y a un an. ServiceNow va ajouter les solutions de BrightPoint à son offre de sécurité qui a été présentée en février dernier. Les deux parties n'ont pas donné de compléments d'informations sur le montant de la transaction.
- **Sopra Steria monte au capital d'Axway.** En raison du désengagement de Géninfo (groupe Société Générale), Sopra Steria monte à hauteur de 33,5 % du capital de l'éditeur Axway, une spin-off de la SSII. Si la société de Pierre Pasquier franchit ainsi le seuil de 30 % du capital, le groupe a obtenu une dérogation de l'AMF et ne se voit donc pas contraint de déposer une OPA sur les titres Axway. Actionnaire de l'éditeur depuis sa séparation de Sopra en 2011, Géninfo cède sa participation de 8,6 % à 21,5 euros le titre, soit un total de 38,6 millions d'euros. A l'issue de cette cession, les actionnaires agissant de concert (Sopra Steria Group, la holding Sopra GMT, les fondateurs et certains managers) contrôlent environ 58,5 % du capital d'Axway et plus de 65 % des droits de vote. Sopra Steria explique cette opération par la volonté de la Société Générale de se désengager de ses participations industrielles. Mi-2015, Géninfo a également soldé sa participation directe dans Sopra Steria (qui représentait 7 % du capital).
- **Les attaques DDoS TFTP sont arrivées.** En mars dernier, nous relations le travail de chercheurs en sécurité sur les risques d'attaques DDoS via des serveurs TFTP, un protocole de transferts simplifié de fichiers. Ils s'étonnaient que cette méthode ne soit pas encore exploitée. Et bien ils n'ont plus à s'étonner puisque Akamai vient de détecter au moins dix attaques DDoS opérées en exploitant TFTP depuis le 20 avril. L'attaque par réflexion (où une requête erronée est renvoyée à la cible et non à son expéditeur d'origine en exploitant les failles du protocole) a permis d'atteindre un pic de 1,2 Gbit/s

pour un volume de paquet de 176 400 paquets par seconde. Rien d'impressionnant en soi mais une charge suffisante pour bloquer le réseau de la cible. Et les attaques risquent de s'amplifier tant que les serveurs faillibles sont en services. Lors de leur découverte, les chercheurs de l'université Napier à Edimbourg estimaient que près de 600 000 serveurs publics avaient laissé leur port 69 (TFTP) ouvert.