DoppelPaymer : ce ransomware « discret » qui n'épargne pas la France

Windows XP, encore bien présent dans les PME françaises ? C'est l'image que renvoie le site « vitrine » de DoppelPaymer.

Ce *ransomware* n'a pas eu, dans l'Hexagone, le même retentissement qu'un Egregor, un Ryuk ou un Maze. Il n'empêche que la liste de ses victimes revendiquées compte une dizaine de références tricolores.

La plus ancienne entrée sur cette liste remonte au 23 février 2020. Elle concerne **Bretagne Télécom**. Son contenu : des informations sur 148 machines (essentiellement les noms d'hôtes, le type de matériel et le système d'exploitation) et quatre archives d'un poids total d'environ 150 Mo. L'entreprise, qui se présente comme un « opérateur de services cloud », n'a jamais communiqué publiquement sur une quelconque cyberattaque qui expliquerait sa présence au sein de la liste.

Il en va de même pour l'**Afpa**. L'organisme de formation professionnelle est la deuxième plus ancienne référence française au rang des victimes. Le butin supposé – publié les 17 et 18 avril – est d'une autre envergure : des informations sur 65 076 machines et près de 4 Go de données, dont certaines possiblement relatives à des projets R&D.

DoppelPaymer : un révélateur de SI

La persistance de Windows XP est particulièrement marquée chez **Roger Martin**. DoppelPaymer semble avoir dérobé au groupe BTP environ 2 Go de données. Une partie d'entre elles paraît impliquer des clients.

Foussier aussi exploitait encore largement Windows XP il n'y a visiblement pas si longtemps. Le distributeur de quincaillerie s'est vu ajouté sur la liste des victimes le 15 octobre. Avec trois archives d'un poids total d'environ 1,5 Go semblant contenir des informations de contact et des contrats.

Dans certains cas, la publication des données s'est faite en deux fois. En l'occurrence, pour **Sparflex** (producteur de packaging pour boissons) et **Amplitude** (groupe de concessions automobiles). Tous deux sont apparus sur la liste des victimes le 9 octobre. Dans un premier temps ne furent publiés qu'une poignée de fichiers, avec un pictogramme qui représentait un mégaphone sonnant comme une menace.
On n'en est effectivement pas resté là. Pour Amplitude, le grand déballage a eu lieu le 20 novembre, avec plus de 4 Go de données. Pour Sparflex, ce fut le 2 décembre (entrée mise à jour le 7), avec environ 1 Go de données.

DoppelPaymer n'épargne pas le secteur associatif. Ainsi l'association **Caminante**, active dans le social et le médicosocial, s'est-elle retrouvée prise au piège. Les quelque 2 Go de données publiés semblent contenir des photos et faire référence à deux noms de famille accompagnés de l'initiale du prénom.

Le butin est moins lourd (environ 100 Mo) aussi bien bien pour **International Container et Transport** (prestataire de services logistiques) que pour **Innelec Multimédia** (distributeur de produits multimédias). Tous deux comptent, sur le périmètre SI auquel DoppelPaymer a pu accéder, une majorité de postes sous Windows 7.

Les collectivités aussi

Seules deux victimes françaises ont officiellement reconnu avoir subi une cyberattaque. Et il s'agit de villes : **Mitry-Mory** (Seine-et-Marne) et **Charleville-Mézières** (Ardennes). Ni l'une ni l'autre n'a mentionné DoppelPaymer, ni même fait allusion à un *ransomware*. Dans les deux cas, néanmoins, la publication du premier communiqué est intervenue quelques semaines avant l'apparition sur le site « vitrine ».

Du côté de Charleville-Mézières, on avait rendu compte des faits le 11 mars, en les situant dans la nuit du 5 au 6. Aucune demande de rançon, nous assurait-on. Avec, dans les grandes lignes, un message : pas de perturbation des principaux services municipaux ; et pour le reste, « tout fonctionne mais par tel [sic] ».

Mitry-Mory avait ouvert la communication le 22 juillet, situant l'attaque à la nuit du 18 au 19. Au fil des semaines, on a notamment appris la perte des archives photographiques de la Ville numérisées depuis le début des années 2000. La liste de 391 machines publiée le 1er octobre sur le site de DoppelPaymer laisse apparaître un parc informatique très hétérogène qui comprend encore du Windows 2000, du XP, du Vista et du Server 2003.

> *[INFORMATION]*
> *Suite à une cyberattaque massive et généralisée les infra-structures informatiques de la collectivité ne…*
>
> *Posted by Ville de Mitry-Mory on Wednesday, July 22, 2020*

Illustration principale © rawpixel.com – Adobe Stock