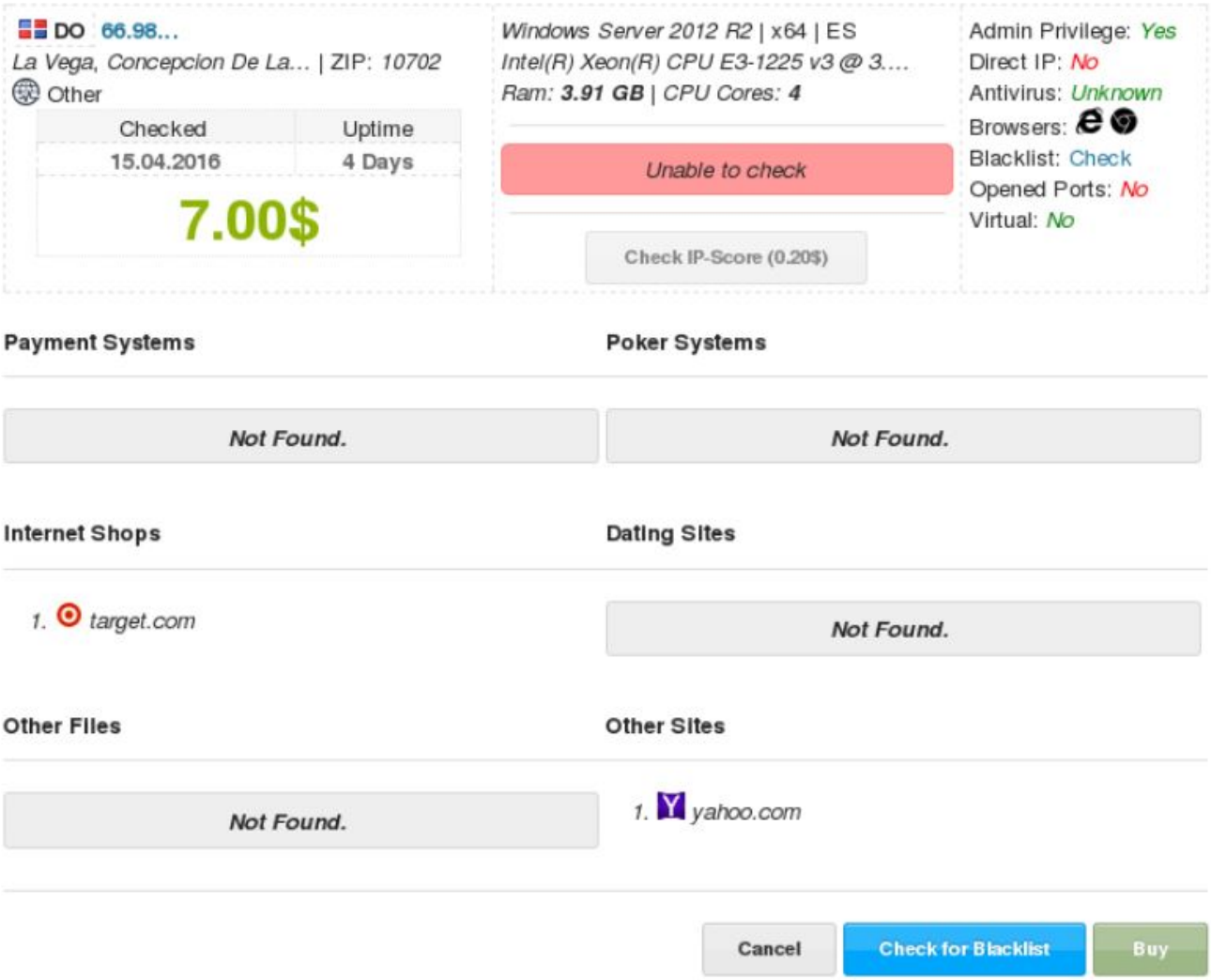
xDedic : une place de marché de 70 000 serveurs piratés

Les codes d'accès d'environ 2 500 serveurs français sont en vente, pour quelques dollars, sur un forum underground, xDedic, accessible depuis un simple navigateur. D'après une étude des laboratoires de l'éditeur Kaspersky, ce sont au total pas moins de 70 000 serveurs Windows compromis, dans 173 pays, qui sont ainsi mis à la portée des cybercriminels. Ces derniers peuvent exploiter ces accès pour lancer des attaques par DDoS, mener des campagnes de spams ou de phishing ou encore accéder aux données présentes sur ces machines. Selon l'éditeur russe, les tarifs démarrent à 6 dollars pour certains serveurs.

L'APT du pauvre ?

« *La vaste quantité de serveurs à vendre sur la place de marché xDedic offre une alternative attractive aux acteurs des APT (Advanced Persistent Threat ou menace persistante avancée) dotés de peu de ressources, mais souhaitant agir sous le radar et ayant des difficultés à prendre pied chez leurs victimes* », écrivent les chercheurs. Bref, une forme de démocratisation des attaques les plus redoutées par les entreprises, celles visant à rester sous le radar afin de récupérer un maximum d'informations confidentielles.



Selon Kaspersky, les administrateurs de ce forum parlent le russe. Les chercheurs de l'éditeur font remonter la naissance de xDedic à 2014. Et dénombrent, en mai 2016, pas moins de 416 individus ou groupes utilisant la plate-forme pour vendre des accès. Le tableau dressé par les chercheurs laisse entrevoir un forum montant en puissance depuis un an et géré avec soin. Le service fournit à ses utilisateurs enregistrés un tableau de bord des serveurs 'disponibles'. Avec, pour chacun d'entre eux, des informations sur la nature du système, la disponibilité d'un accès administrateur, la présence d'antivirus ou de navigateurs, la vitesse de connexion ou encore le tarif et la localisation. Sans oublier la présence ou non de logiciels de gestion des terminaux point de vente, une information cruciale pour les spécialistes du vol de données de cartes bancaires.

Un portail 'clients', un portail 'vendeurs'

Autre illustration de la spécialisation et de la professionnalisation des différentes composantes du cybercrime : xDedic propose un portail 'partenaires', comprendre une interface dédiée aux vendeurs de serveurs compromis. Protégée par login et mot de passe, celle-ci renferme un outil de validation, SysScan, qui établit le profil des machines appelées à être proposées à la vente. L'outil se connecte à des serveurs de commande et de contrôle, afin de transmettre des informations précises sur la cible (identifiant du serveur, version de Windows, langue, taille de la mémoire, CPU, ouverture des ports 25 et 80, présence d'environnements virtuels, antivirus…) que xDedic va afficher dans son portail 'clients'. SysScan effectue également quelques modifications dans

Windows, facilitant l'exploitation du serveur compromis.

xDedic « *facilite la vie de ses clients* »

D'après les conclusions de Kaspersky, les serveurs sont piratés par force brute, en utilisant des outils ciblant le protocole RDP (Remote Desktop Protocol, protocole d'accès à distance venant du monde Windows), comme DUBrute ou XPC. Puis, xDedic intervient comme une suite de services permettant d'industrialiser l'exploitation de ces ressources et d'en organiser la commercialisation. Ainsi, en attendant qu'un serveur soit 'acheté' sur la place de marché, les hackers le détournent pour réaliser du minage de bitcoin. Autres signes de la sophistication des processus mis en place par xDedic : la présence d'un client RDP développé en propre et « *conçu pour faciliter la vie de nos clients* » selon les mots de l'organisation criminelle ou encore un outil maison permettant de transformer un serveur en proxy (HTTPS ou Socks).

Notons par ailleurs que les chercheurs de Kaspersky sont parvenus à détourner le trafic de 5 des 8 serveurs de contrôle utilisés par xDedic pour piloter les serveurs via le malware SCClient. « *Au cours des 12 premières heures, nous avons reçu des connections de 3 600 adresses IP différentes* », écrivent les chercheurs. Ce qui donne une idée du niveau d'activité réelle de cette organisation cybercriminelle. Kaspersky affirme que des serveurs d'organisations gouvernementales ou d'universités faisaient partie des machines se connectant aux serveurs de contrôle.

A lire aussi :

CryptXXX : le ransomware qui vole aussi les mots de passe

Sécuriser les Scada : « ce sera cher et difficile », dit Kaspersky

Hacking : pourquoi les États s'en prennent aux éditeurs de sécurité

Crédit photo : igor.stevanovic / shutterstock