La France fait face Ã une nouvelle cyberattaque
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 15/3/2024 14:00:00

Alors que plusieurs services de l'Etat ont fait l'objet de cyberattaques il y a seulement quelques jours, la France fait face Ã une nouvelle cyberattaque Ã lâ□□encontre dâ□□un organisme public. France Travail a en effet rÃ©vÃ©lÃ© avoir Ã©tÃ© la cible de cybercriminels, avec Â« un risque de divulgation Â» de donnÃ©es personnelles touchant Â« potentiellement Â» 43 millions de personnes.

Dirk Schrader, Resident CISO (EMEA) et VP of Security Research chez Netwrix a fait le commentaire suivant :

Â« Les organismes publics sont souvent pris pour cible dans le seul but de provoquer le dÃ©sordre. Les cybercriminels savent qu'il est peu probable qu'ils obtiennent une ranÃ§on Ã la suite d'une telle attaque.

Ils y voient plutÃ´t une preuve publique de leur capacitÃ© Ã la mener Ã bien et un moyen de rÃ©colter une quantitÃ© massive de donnÃ©es personnelles vÃ©rifiÃ©es pour les exploiter ensuite. Pour simplifier, les cybercriminels Â« montrent leurs muscles Â» lors de ces attaques pour dÃ©couvrir les TTP (tactiques, techniques et procÃ©dures) qui fonctionneront dans la nature avant de les appliquer Ã une cible plus sophistiquÃ©e.

L'origine de ces attaques - des vulnÃ©rabilitÃ©s exploitÃ©es ou des informations d'identification compromises - est souvent due Ã des infrastructures obsolÃ¨tes et Ã des processus de sÃ©curitÃ© inadÃ©quats. Un autre exemple de ce type d'attaque est celui du district allemand d'Anhalt-Bitterfeld.

Elle a entraÃ®nÃ© l'arrÃªt de l'administration complÃ¨te du district, qui compte 160 000 citoyens, et a finalement engendrÃ© des coÃ»ts de rÃ©cupÃ©ration de 2,5 millions d'euros, bien qu'aucune ranÃ§on n'ait Ã©tÃ© payÃ©e.

Les deux attaques rÃ©centes, l'attaque DDoS sur les rÃ©seaux du gouvernement franÃ§ais et l'attaque qui a visÃ© France Travail exploitant des informations d'identification compromises, comportent un autre aspect notable.

Les cybercriminels savent comment exploiter les grands Ã©vÃ©nements mondiaux et ce dont ils ont besoin pour se prÃ©parer Ã une telle exploitation. A l'approche des Jeux olympiques de 2024, l'accÃ¨s aux donnÃ©es personnelles vÃ©rifiÃ©es d'environ 43 millions de franÃ§ais ressemble Ã une campagne de prÃ©paration Ã d'autres attaques.

Nous pouvons nous attendre Ã des campagnes de phishing sur mesure, par exemple, pour des demandeurs d'emploi potentiels autour d'offres d'emploi liÃ©es Ã l'Ã©vÃ©nement et Ã des tentatives de soutirer de l'argent aux destinataires, comme "Inscrivez-vous Ã une base de donnÃ©es spÃ©ciale d'offres d'emploi olympiques".

En outre, les campagnes de phishing menÃ©es dans ces bases de donnÃ©es peuvent viser Ã collecter des mots de passe ou des numÃ©ros de tÃ©lÃ©phone mobile potentiellement rÃ©utilisÃ©s afin de dÃ©jouer les processus d'autorisation de transfert de fonds par SMS Â».