Egyre olcsóbbak a lopott jelszavak, ami nem jó jel

Biztonsági kutatók szerint a feketepiacokon egyre több RDP hozzáférést kínálnak eladásra, ami az árak csökkenésével a kibertámadásokat is egyre olcsóbbá teszi.

A kiberbűnözők egyre olcsóbban kínálják a céges hálózatokhoz való azonosítókat és az általában a rendszeradminisztrátorok által használt RDP (remote desktop protocol) hozzáféréseket, ami nem csak azt jelzi, hogy a hekkerek is egyre könnyebben férhetnek hozzá az ilyen felhasználónév-jelszó kombinációkhoz, de azt is mutatja, hogy a jelszavak hagyományosan csapnivaló kezelése a világjárvány és a tömeges távmunka korszakában a korábbinál is nagyobb problémát jelent.

Néhány héttel ezelőtt a a Webroot statisztikáját idéztük, amely szerint a távoli gépekhez csatlakozó, azok grafikus felületét használó eszközök száma 40 százalékkal növekedett a járvány kezdete óta, ráadásul még ezen belül is emelkedik a nem biztosított RDP-k aránya. Ehhez képest Have I Been Pwned szolgáltatásában összegyűjtött, igazoltan kompromittált belépési információk elemzéséből már az is kiderült, hogy a teljesen egyedi jelszavak az összes karaktersor egytized részét sem teszik ki, és ezek között is csak egy kisebb részt képviselnek a teljesen értelmetlen jelszavak.

Az Armor kiberbiztonsági kutatói összesen 15 feketepiacot fésültek át a dark weben és az ehhez kapcsolódó bűnözői fórumokon, így jutva arra a megállapításra, hogy az RDP hozzáférések átlagos ára esetenknt már 16 dollár közelébe csökkent, szemben az előző évi 20 dollárral. Egyes eladók még a „non-hacked" címkével is ellátják az árujukat, jelezve, hogy az általuk kínált azonosítókat még sohasem használták fel hasonló célokra.

A legtöbb lehetőséget ajándékba kapják

A ZDNet beszámolója szerint az ilyen adatok legelsősorban azért kerülhetnek a hekkerek kezébe, mert eleve rosszul biztosították azokat: a felhasználónevek olyan könnyen megtippelhető kifejezések, mint mondjuk az „administrator", és a jelszavak is sokszor gyakran használt, kifejezetten gyenge karaktersorok. Ezeket esetenként az automatizált brute force támadások is gond nélkül feltárják, vagyis próbálgatással is viszonylag hamar megtalálhatók, a bűnözők pedig eldöntik, hogy maguk akarják kihasználni a hálózatokhoz szerzett hozzáférést, vagy eladásra kínálják az információt.

Mivel ezek a hozzáférések akár olyan nagyszabású malware vagy ransomware támadásokra is alkalmat adhatnak, amelyekről az utóbbi időben egyre gyakrabban vagyunk kénytelenek beszámolni, az árak folyamatos csökkenése nagyban hozzájárul a probléma súlyosbodásához. Ez ugyanis értelemszerűen azt jelzi, hogy a feketepiacon már a kínálati oldal dominál, ahogy egyre több és több azonosító jelenik meg rajta, és ezzel a támadások költségei is egyre alacsonyabbak.

Ez a trend nyilván erősen kapcsolódik a távmunka erőltetett és széleskörű bevezetéséhez, a szakemberek szerint azonban nincs a dologban semmi sorsszerűség: mindössze két egyszerű szabályt betartva már töredékére csökkenthetnénk a kockázatokat. Egyrészt minden szervezetnél szigorúan ellenőrizni kellene, hogy semmilyen fiókot nem az alapértelmezett belépési kulcsokkal biztosítanak, és a céges felhasználókat is ösztönözni kellene a minél erősebb jelszavak alkalmazására. Másrészt ahol csak lehet be kellene vezetni a többfaktoros azonosítást, ami nagyban akadályozná a bűnözőket, hogy a gyakorlatban kiaknázzanak egy megszerzett név-jelszó párosítást.

Forrás: https://bitport.hu/egyre-olcsobbak-a-lopott-jelszavak-ami-nem-jo-jel

Válogatta: Fonyó Istvánné