Már egyenesen a felhőből jön egy nagy csomó kártevő

A Netskope legfrissebb statisztikája alapján nem csak a támadók egyre aktívabbak, de a munkahelyi felhasználói gyakorlatok is komoly kívánnivalókat hagynak maguk után.

A Netskope kiberbiztonsági cég adatai szerint a felhőszolgáltatásokon keresztül továbbított rosszindulatú programok mennyisége több mint kétharmadával, 68 százalékkal növekedtek az idei második negyedévben az előző év megfelelő időszakához képest. A társaság legutóbbi Cloud and Threat Report című jelentése alapján ezen belül is a felhő alapú tárolási megoldások viszok a prímet, amelyek az összes ilyen malware terjesztésének több mint 66 százalékáért felelősek.

A hálózati és biztonsági funkciókat egyesítő (Secure Access Service Edge, SASE) cloud platformot fejlesztő Netskope ötödik alkalommal tette közzé a felhőben kezelt adatok kockázatait, illetve az ilyen fenyegetéseket és trendeket feldolgozó riportját. Eszerint 2021 második negyedévében az összes rosszindulatú program letöltésének 43 százaléka valamilyen rosszindulatú Office-dokumentumhoz kapcsolódott, szemben a 2020 eleji 20 százalékkal, ami egyebek mellett azt jelzi, hogy sokan próbálkoznak az időközben felszámolt Emotet banki trójai és annak üzemeltetői által alkalmazott technikákkal.

A rosszindulatú kódok terjesztésének második legnagyobb csoportját a kollaborációs alkalmazások és fejlesztőeszközök teszik ki, miután a támadók egyre gyakrabban használják fel erre a célra a népszerű üzenetküldő alkalmazásokat és repository-kat. Ahogy nemrég például a Kaspersky saját adataiból is kiderült, a társaság androidos biztonsági alkalmazása napi átlagban majdnem 500 kártékony hivatkozást fog az üzenetküldő appokban, amelyeket már 2,7 milliárd ember használ világszerte.

A felhasználók is mindent megtesznek

A Netskope 2021 első felében összességében 290 féle különálló felhős alkalmazásban észlelte és blokkolta a rosszindulatú programok letöltését. A vállalat kutatói szerint egyébként az összes ilyen munkafolyamat körülbelül 35 százaléka férhető hozzá valamilyen módon a nyilvános internetről az Amazon (AWS), a Microsoft (Azure) vagy a Google (GCP) platformjain, és érhető el a világhálóról bárhonnan nyilvános IP-címmeken keresztül.

A jelenlegi feltételek között nem meglepő, hogy a távoli asztali protokollok (RDP) egyre gyakoribb támadási vektornak számítanak. A Netskope szerint egy átlagos, 500-2000 alkalmazottal működő szervezet 805 darab különálló alkalmazást és felhőszolgáltatást használ, amelyek 97 százalékát nem menedzseli megfelelően, és azokat gyakran szabadon alkalmazzák az üzleti egységek és a céges felhasználók. Márpedig az ilyen applikációk gyors ütemű bevezetése az idén is folytatódik, a Netskope adatai alapján az év első felében 22 százalékkal nőtt a tavalyi szinthez képest.

A jelentése felhívja rá a figyelmet, hogy a munkavállalói szokások önmagukban is jelentős kockázatokat hordoznak ezen a téren, legyen szó az irodai vagy az otthoni munkavégzésről. Ez megmutatkozik a harmadik féltől származó alkalmazások engedélyezésében vagy az olyan jelenségekben, hogy a szervezetekből kilépő alkalmazottak az utolsó 30 munkanapjuk során háromszor több adatot töltenek fel személyes alkalmazásaikba, mondjuk a Google Drive-ra vagy a Microsoft OneDrive-ra. Mivel ezek az esetek legalább 15 százalékában valamilyen belső, menedzselt alkalmazásból származó adatok közvetlen másolatai, nem kérdés, hogy ilyenkor a meglévő céges adatkezelési szabályok is sérülnek.

Forrás: https://bitport.hu/mar-egyenesen-a-felhobol-jon-egy-nagy-csomo-kartevo

Válogatta: Fonyó Istvánné