filter:max
az erőforrásbiztonsági cég

Account takeover monitoring rendszer

Account takeover (ATO)

A account takeover a szervezethez kapcsolódó, a szervezet felhasználói által igénybe vett belső és külső szolgáltatások hozzáféréseinek kompromittálódását jelenti.

Az incidens során egy vagy több, külső vagy belső rendszerhez hozzáférő felhasználó bejelentkezési azonosítója és jelszava illetéktelen kézbe jut, bizalmassága súlyosan sérül.

Account takeover esetén a kiszivárgott hozzáférés segítségével illetéktelen személyek is hozzáférhetnek az adott szolgáltatáshoz vagy rendszerhez. Az eseményből más incidensek is következhetnek, mivel a felhasználók jellemzően azonos vagy csak nagyon kismértékben eltérő jelszavakat használnak az egyes szolgáltatásokhoz, tehát ha egy hozzáférés kompromittálódik, lehetséges, hogy más szolgáltatásokba is be tud jelentkezni az illetéktelen személy.

Még súlyosabbá válhat a probléma, ha a szervezeten belül a belső rendszerekhez történő hozzáférésekhez használja a felhasználó a kiszivárgott jelszót, és a belső jelszócsere folyamatok hosszú átfutásúak (60-90 nap).

Ilyen eset lehet, amikor a felhasználó az egyszerű megjegyezhetőség miatt ugyanazt a jelszót használja a VPN bejelentkezéshez (AD login), mint amelyet például a külső szolgáltatás esetében (pl. LinkedIn).

Sok esetben a nyilvános szolgáltatások feltöréséről csak hosszú hónapokkal később jelenik meg nyilvános információ, a publikálásig eltelő időszakban azonban a megszerzett felhasználói azonosítók és jelszavak a feketepiaci adásvételek egyik legfontosabb árucikke.

Mire a szervezet értesítést kap a szolgáltatás kompromittálásáról, az eltelt időszakban a támadók által megszerzett vagy megvásárolt, a szervezet felhasználóihoz kapcsolódó bejelentkezési adatok potenciális veszélyforrást jelentenek.

A problémára és vakfoltra az **account takeover (ATO) monitoring** jelenthet megoldást.

filter:max
az erőforrásbiztonsági cég

SpyCloud- ATO monitoring

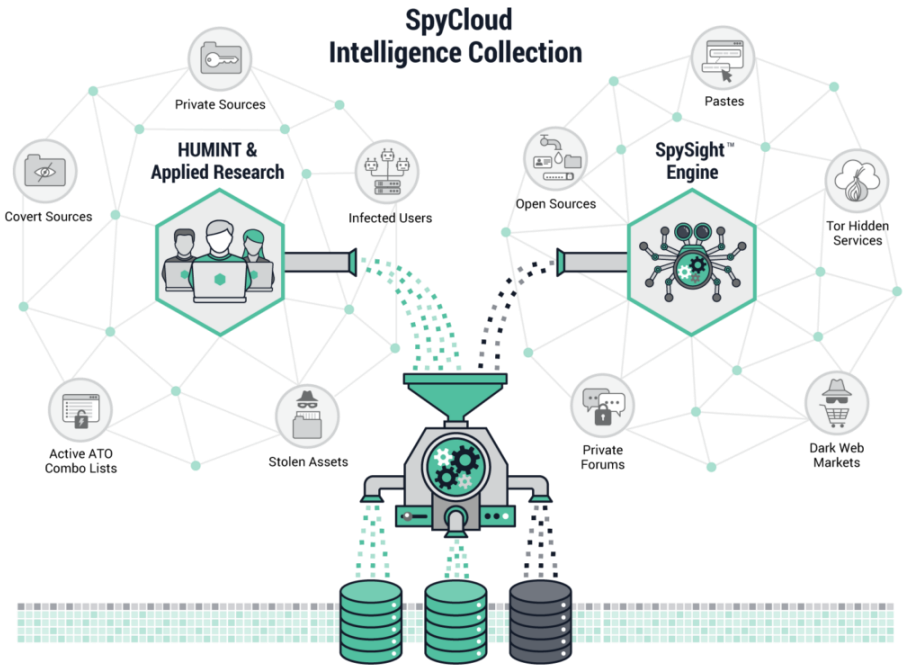
A Secure Networx Kft. a SpyCloud ATO monitoring platformot használja és javasolja az esetlegesen kiszivárgott hozzáférések felderítésére és monitorozására.

SpyCloud

A SpyCloud szolgáltatás ötvözi az OSINT és HUMINT felderítési módszertanokat, azaz a nyilvános forrású hírszerzés mellett emberi erőforrás-alapú felderítést is végez.

Az OSINT folyamatokban a már korábbi támadásokból és hackelésekből származó, már publikálásra került felhasználói információkat aggregálják és dolgozzák fel. (az ingyenesen elérhető rendszerekből jelenleg csak felhasználóként lehet lekérdezni, a SpyCloud rendszerében azonban a teljes szervezettel kapcsolatos összes érintett adat és információ egyszerre jelenik meg).

A HUMINT folyamat során a gyártó fedett „ügynökei" a feketepiaci és DARKNET területeken élőerős felderítési műveleteket végeznek, valamint mint „potenciális vásárlók" áruba bocsátott felhasználói adatbázisokat vásárolnak és szereznek meg, majd dolgoznak fel.

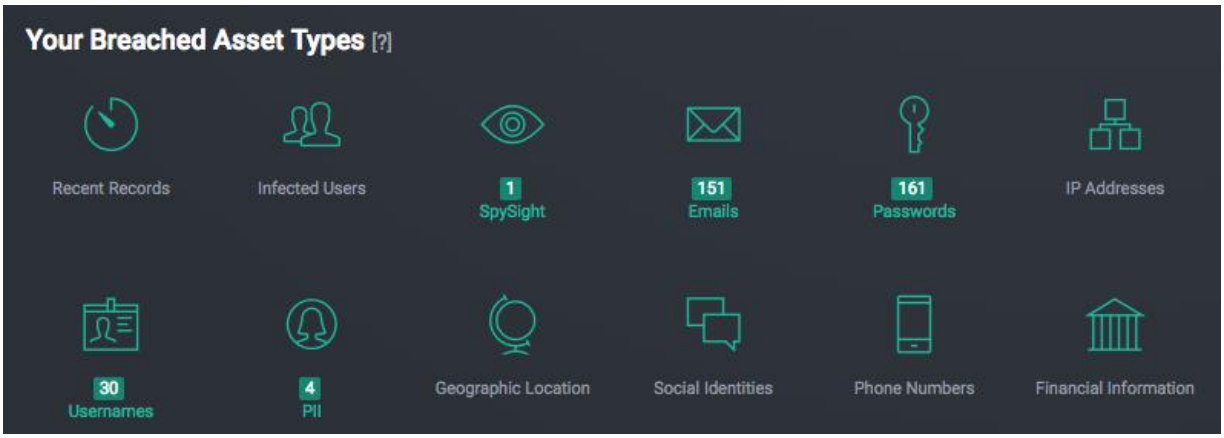


Account Takeover Monitoring

filter:max
az erőforrásbiztonsági cég

Hogyan működik?

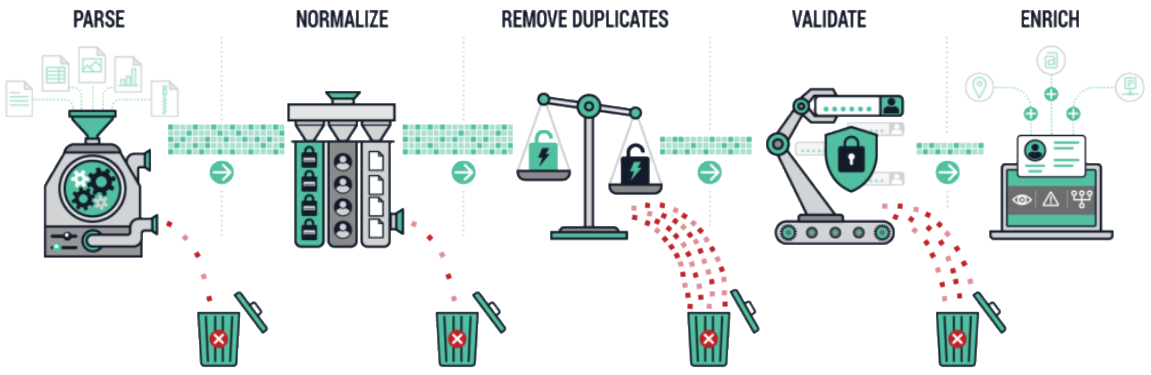
A rendszer használatához a menedzsment felületen csak a szervezethez tartozó domain címeket kell konfigurálni, valamint meg kell adni a riasztási és email címet, ahova a rendszer riasztást küld, ha valamely szervezethez köthető és kompromittálódott hozzáférést fedez fel.



Adott domainhez köthető kiszivárgott felhasználói hozzáférések és adatok

A SpyCloud folyamatosan monitorozza a nyilvános vagy előfizetéshez kötött ATO forrásokat, valamint a HUMINT folyamatokban begyűjtött, esetleg a feketepiacon vagy a DARKNET-en megszerzett vagy megvásárolt felhasználói adatokat.

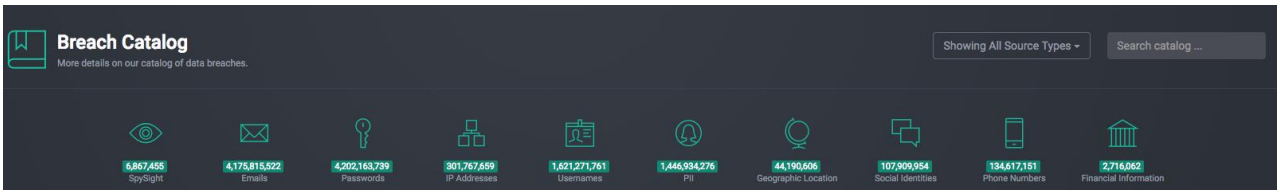
A SpyCloud szakemberei automatikus és manuális tisztítási folyamatokkal és ellenőrzésekkel dolgozzák fel a begyűjtött adatokat, ezzel biztosítva, hogy a rendszer jó minőségű adatokkal dolgozzon.



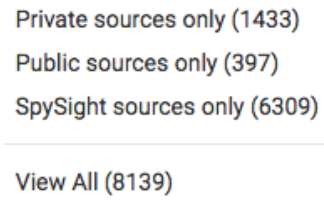
Tisztító és ellenőrző folyamatok

Account Takeover Monitoring

A SpyCloud szakemberei a megszerzett és letisztított információkat folyamatosan töltik be a rendszerbe, így, ha olyan felhasználói adat kerül bírtokukba, amely a szervezet felkonfigurált domain címéhez köthető, a rendszer azonnal riasztást küld a beállított értesítési címre.



Breach Catalog, 4 milliárd rekord feletti adatmennyiség



Több, mint 8000 adatforrás

A SpyCloud jelenleg több, mint 8000 adatforrásból gyűjti az információkat, és több, mint 4 milliárd kompromittált felhasználói rekordot tartalmaz.

A SpyCloud előnye az ingyenes szolgáltatásokhoz és más gyártók megoldásához képest, hogy a monitoring folyamat nem scannelésen (PasteBin, stb.) alapul, hanem valós HUMINT felderítő tevékenységen.

A SpyCloud nem csak a már nyilvánosságra került információkkal dolgozik, hanem a fedett tevékenységein keresztül már akkor is képes észlelni a szivárgást, ha az adott incidens még nem is került nyilvános publikálásra.

A SpyCloud egyedi funkciója, hogy ha SHA1 vagy más hash-alapú jelszó kiszivárgását észleli, egyrészt ellenőrzi azokat a nyilvános *hash killer* (pl. https://hashkiller.co.uk/) adatbázisokban, illetve megpróbálja saját maga is visszaállítani a hash-elt jelszót.

Ha olyan kiszivárgott jelszó hash-t észlel, amelyet a nyilvános hash-törő alkalmazások már ismernek (tehát valaki már feltörte), vagy ha a saját rendszere képes a jelszót visszaállítani (tehát a jelszó gyenge és megfejthető), kiemelt prioritású figyelmeztetést tud küldeni.

Account Takeover Monitoring