CTI Jelentés

Jelszó trendelemzés

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

Bevezetés

Jelszavak és kódok használata informatikai rendszerek védelmére a 60-as évekre vezethető vissza. Azóta is ezek jelentik a legelső védelmi vonalat rendszereink, fiókjaink és adataink biztonságba tartásához. Azonban a technológiai fejlődés és a kiberbűnözők módszertani tárházának bővülése rávilágít minket arra, hogy az általunk használt jelszavak sem mind egyenlőek, ha a biztonságról van szó.

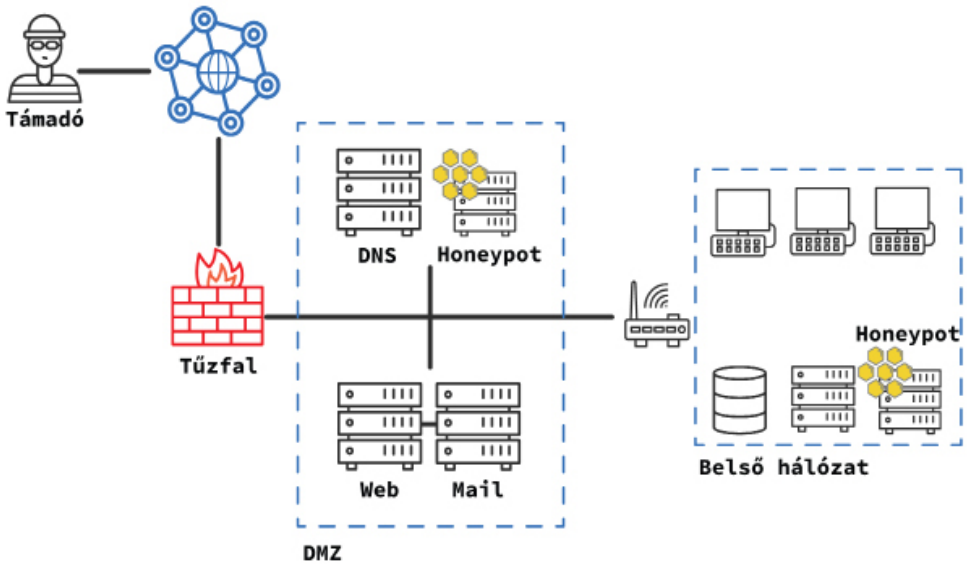
Az erős és változatos jelszóhasználat kulcsfontosságú az alapvető kiberhigiénia fenntartásához. Egy rosszul választott jelszó magas kockázatot jelent, amely könnyen a bizalmasság kárára fordulhat.

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Kormányzati Elosztott Hálózatbiztonsági Csapdarendszer (GovProbe) szolgáltatása nap mint nap gyűjti az illetéktelen behatolási kísérletekből származó értékes adatokat. A különböző csapdák elterjedt informatikai szolgáltatásokat imitálnak, amelyek képesek interakcióba lépni a támadókkal. A jól monitorozott és hálózatilag elkülönített környezet minden cselekményt rögzít, így mélyebb betekintést nyerhetünk a kiberbűnözők módszereibe.

***A csapdarendszerek** — vagy angol nevükön **honeypotok** — **félaktív hálózatbiztonsági technológiák, amelyek csaliként szolgálnak a támadások elterelésére.** Felhasználásuk igen sokrétű, egyrészt „időt nyerhetnek" a támadott infrastruktúra üzemeltetői számára, hogy észleljék a hálózat kompromittálódását, másrészt a támadók módszereinek tanulmányozása kutatásokhoz is felhasználható.*

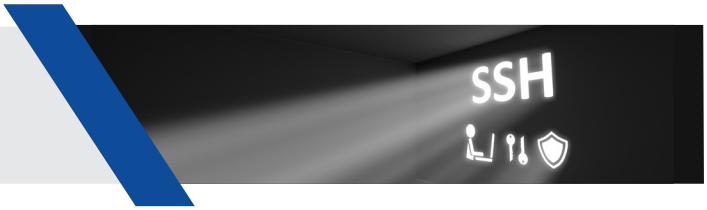
Az NBSZ NKI a GovProbe csapdarendszerekből érkező adatokat feldolgozza, amelyből különböző riasztások és trendelemezések készülnek *a közigazgatási szervek és vállalatok számára. Az Intézet CTI programjával kiegészítve a szervezetek naprakész képet kaphatnak a kibertér fenyegetéseiről. A különböző szolgáltatások között az SSH csapdák különlegessége, hogy a támadók felhasználónév és jelszó párosokkal tesznek bejelentkezési próbálkozásokat, amelyeket a rendszer eltárol.*

Az NBSZ NKI Eseményészlelési Szakterültete 100 000 elkülöníthető, a GovProbe csapdarendszer felé irányuló behatolási kísérletből kinyert jelszavakból különböző elemzéseket készített, amelyekből pontosabban megismerhetjük miként is használják fel a bűnözők becses jelszavainkat.



Csapdarendszer működése

SSH statisztikák



A Secure Shell, avagy SSH egy, az informatikában bevett és széles körben használt protokoll, amely hálózati összeköttetésen keresztül képes titkosított kapcsolatot felépíteni egy másik számítógéppel. A főleg rendszer-adminisztrációs célból használt SSH protokoll által hozzáférhetünk akár a cél szerver teljes adatállományához és erőforrásaihoz. Pontosan ezen funkciója miatt kifejezetten értékes célpont a kiberbűnözők számára. Ahhoz, hogy az SSH kapcsolat létrejöjjön, szükséges valamilyenféle felhasználó bejelentkezést végbe vinni, amely gyakran kimerül a felhasználónév jelszó kombinációban.

Érdemes megjegyezni, hogy manapság az SSH esetében a ***kizárólagosan felhasználónév-jelszó kombinációt használó hitelesítési megoldás nem számít biztonságosnak****, így fontos, hogy amennyiben SSH szolgáltatást futtatunk, mindenképpen alkalmazzunk kétfaktoros és kulcsalapú hitelesítést is.*

Az SSH csapdákra 2021 és 2022 között beérkezett, 100 000 vizsgált esemény közül 28 874 egyedi jelszót és 25 632 felhasználónevet sikerült azonosítani. Összesítve mind a jelszavaknál, mind a felhasználóneveknél a választás leggyakrabban az alapértelmezett rendszerbeállításokhoz köthető szavakra esett. Gyakori és tipikus rossz gyakorlatnak számít, amikor egy rendszeradminisztrátor a könnyű megjegyezhetőség alapján választ jelszót, vagy meghagyja a gyári beállításokból származó hitelesítési adatokat. Ilyenek lehetnek például az „admin", a „root", a „support", a „test" és ezek különböző, kreatívabbnál kreatívabb megfelelői.

Habár ezek tekinthetőek a legegyszerűbb próbálkozásoknak, sajnos nem hiába ezek jelennek meg legnagyobb számban. A tapasztalatok azt mutatják, hogy a mai napig nagy számban fordulnak elő gyári beállításokkal ellátott rendszerek, amelyek rossz konfiguráció miatt elérhetőek a nyílt Internet felől.

A gyenge jelszóhasználat kihasználhatóságára és az abból fakadó veszélyekre tökéletes példa az Egyesült Államok kormányzati rendszerei elleni kibertámadás, amelyet az egyik beszállítójukon, a SolarWinds vállalat szoftverein keresztül vittek végbe állami támogatású hackerek 2019 és 2020 decembere között. Az incidensről szóló jelentések alapján a támadásban egy gyenge jelszó központi szerepet játszott. A nagy port kavart incidenssel mélyebben is foglalkoztunk egy korábbi kiberbiztonsági elemzésünkben.

Az elemzett események alapján a támadók előszeretettel használják próbálkozásaikhoz a számsorrendből álló jelszavakat, azoknak hosszabb és rövidebb formáit *(pl.: 123456, 12345, 123)*. Természetesen nem beszélhetünk gyenge jelszavakról anélkül, hogy meg ne említenénk a jelszó angol megfelelőjének *(password)* különböző használatát. **A teljes tartomány közel 2%-a pass szó valamilyen variációjából állt.** Ebből is láthatjuk, hogy az úgynevezett bevett és tipikusnak mondható jelszavak igencsak népszerűek és gyakran az elsők között állnak a fiókfeltörési kísérletek során.

A támadók által felhasznált jelszavak sokat elárulhatnak az átlagfelhasználók jelszóhasználati szokásairól is. Habár a jelszókezelő alkalmazások és velük együtt a komplexebb jelszavak használata egyre szélesebb körben ismert, sajnos a statisztikák általánosságban azt mutatják, hogy a gyenge, könnyen feltörhető, számokat és speciális karaktereket mellőző jelszavak használata gyakori és elterjedt hiba.

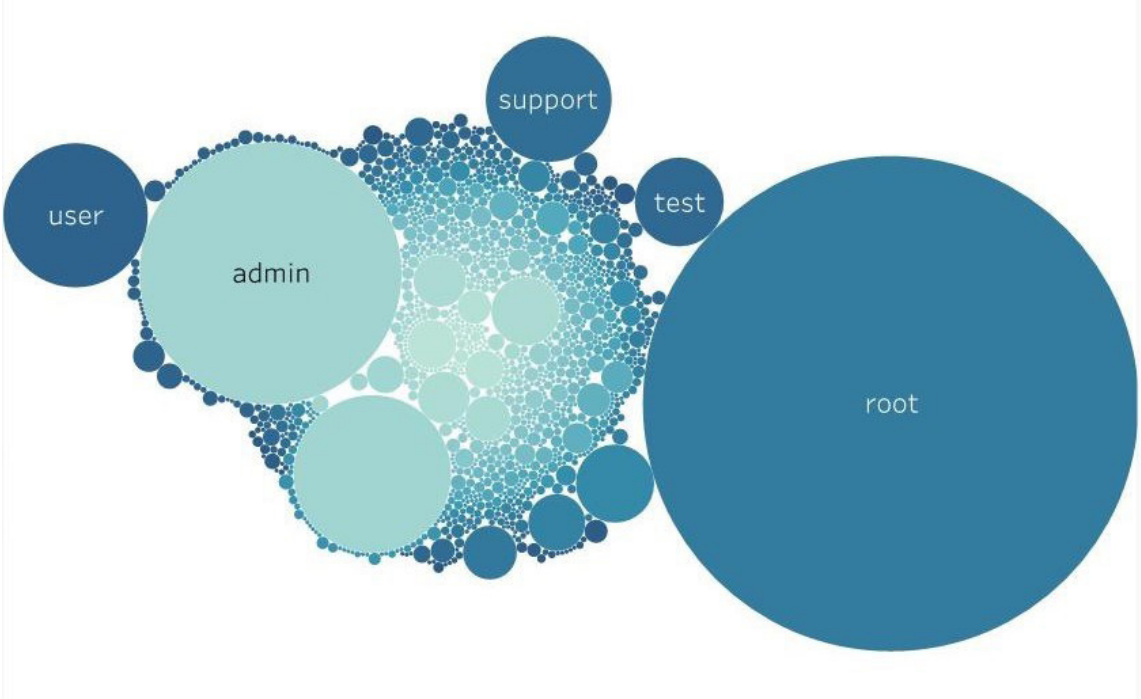
Az SSH csapdákra beérkező adatok közül egy szűrés kimutatta, hogy az erős jelszó kategóriának megfelelő jelszavak csupán 3%-át adták ki a teljes tartománynak. Ez azt mutatja, hogy **a támadók inkább a gyengébb, egyszerűen kitalálható jelszavakkal próbálkoznak, az erősebb jelszavakra kitalálására az esély igen csekély.** Ebből is látszik mennyire fontos, hogy **jelszavainkat mindig átgondoltan, sokkal inkább a biztonságot, semmint a kényelemet szem előtt tartva alkossuk meg.**

TIPP

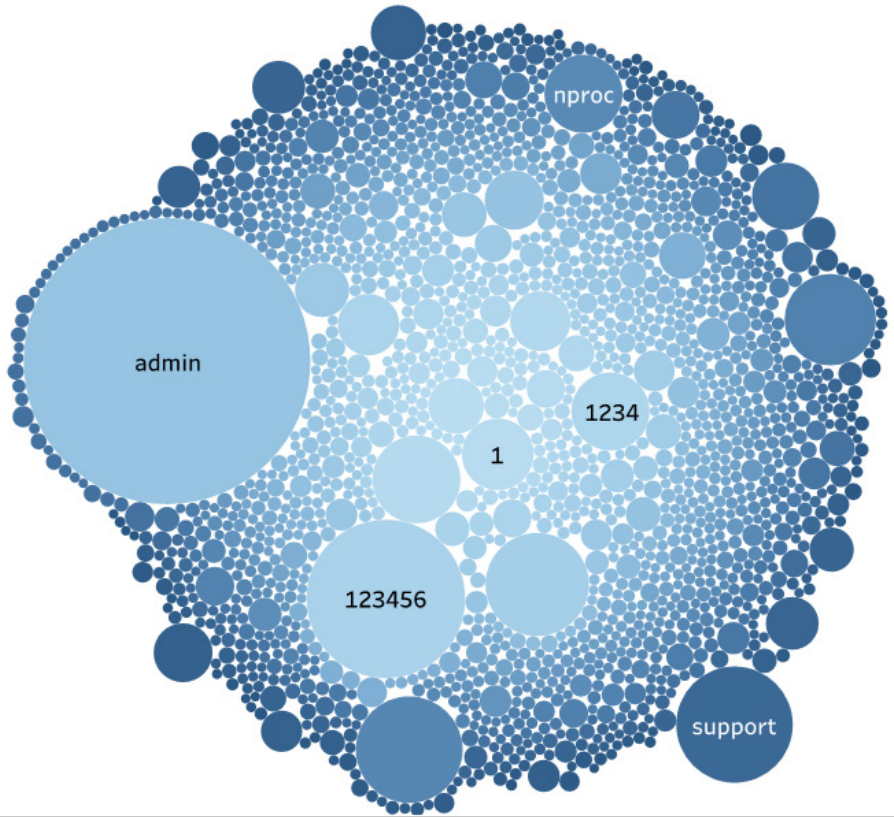
A biztonságos jelszó a következő tulajdonságokkal rendelkezik:

- *minimum 12 karakter hosszú;*
- *vegyesen tartalmaz kis- és nagybetűket, illetve számokat;*
- *tartalmaz speciális karaktereket;*
- *nem tartalmaz számsorozatokat (pl.: 123456) és ismétlődéseket (pl.: 112233).*

Érdemes megtekinteni a vizsgált jelszavak és felhasználónevek frekvenciájában tapasztalható különbségeket. Összesítve láthatjuk, hogy a legnépszerűbb szavak arányaiban kiugró mértékekben dominálnak. Ez megmutatja, hogy a támadók a legvalószínűbb bemeneti értékekkel próbálkoznak, főleg a legóvatlanabb áldozatokat célozva ezzel. Mindez kifejezetten jellemző a felhasználónevek terén, ahol a támadók az alapvető *root* és *admin* belépési adatokkal próbálkoznak leginkább. Jelszavak esetében az egymás közötti méretkülönbség aránya egyenletesebb. Néhány kiugró értékek mellett (például az *admin* és az *123456*) nagyobb mennyiségben található meg a különlegesebb egyszer vagy kis mennyiségben használt jelszavak.

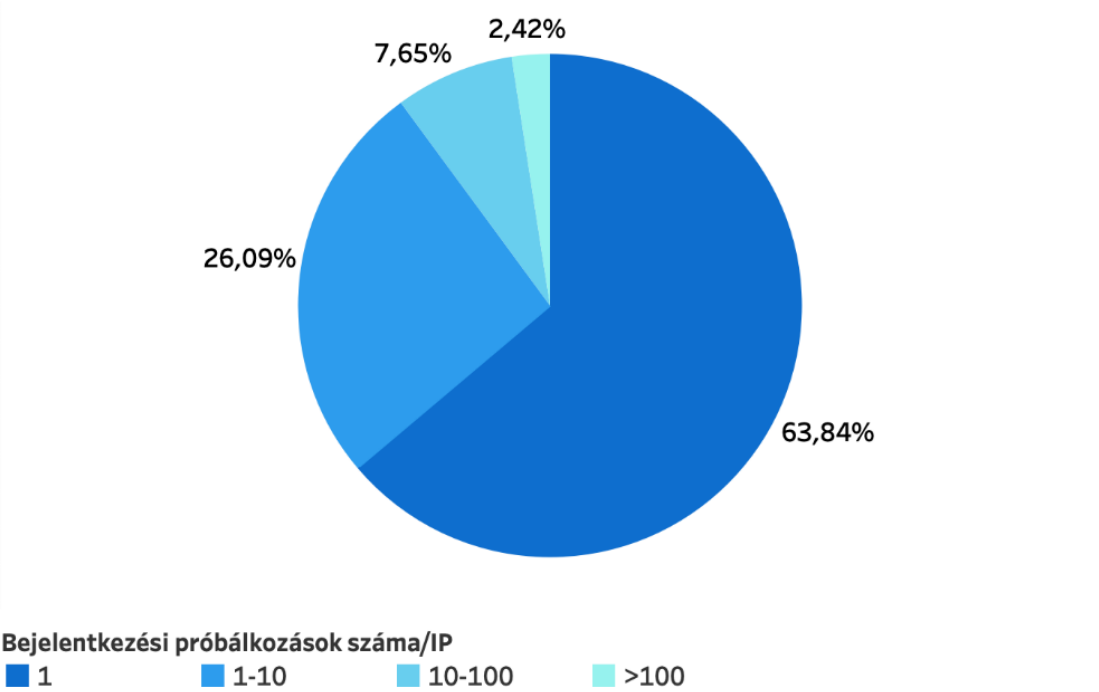


Felhasználónév előfordulások mértéke



Jelszó előfordulások mértéke

A jelszavak és felhasználónevek frekvenciájának értelmezéséhez érdemes mélyebben betekintenünk az egyes támadások körülményeibe. Amennyiben lebontjuk az SSH csapdára beérkezett próbálkozásokat forrás IP címre, felfedezhetjük, hogy nagy arányban, (64%-ban) különálló IP címekről indultak a behatolási kísérletek. Ez a nagy szám automatizált támadásokra, ún. „botokra" (robothálózat) utal, amelyek minél nagyobb áldozatsprektumot akarnak elérni.



SSH bejelentkezési kísérletek száma IP címekre bontva

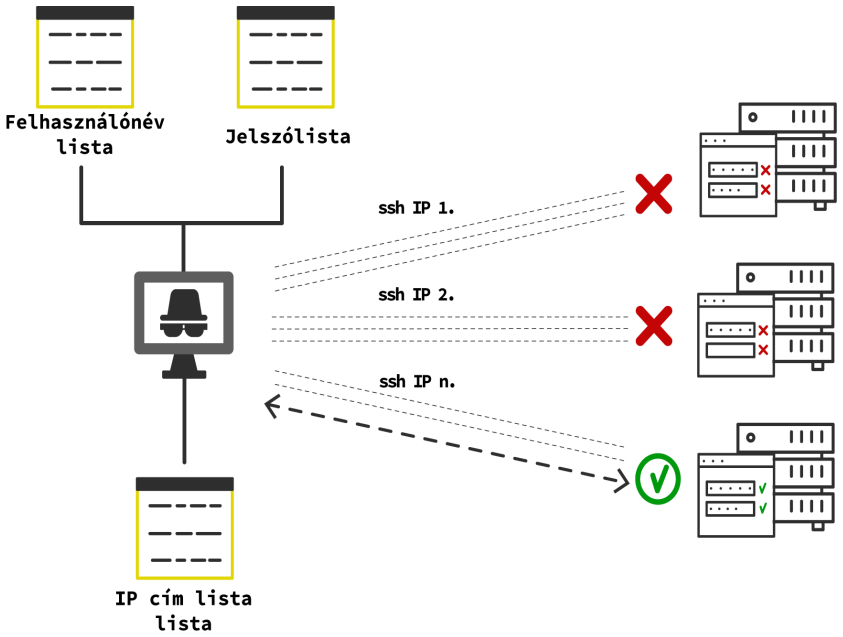
TOP 20 JELSZÓ ÉS FELHASZNÁLÓNÉV

Amennyiben a tiéd is közte van, akkor ideje megváltoztatni!

	FELHASZNÁLÓNÉV			JELSZÓ	
1	root	11	123321	admin	root
2	admin	12	1234	123456	12345
3	Administrator	13	0	support	123
4	user	14	!root	P@Ssw0rd	admin123
5	support	15	22	12345678	user
6	test	16	adm	PassWord	0
7	nproc	17	123	1qaz@WSX	ubnt
8	111111	18	ftpuser	1234	abc123
9	pi	19	info	nproc	test123
10	sales	20	guest	1	test

A GovProbe csapdarendszerekbe érkező támadások tehát leggyakrabban automatizáltak. Ez azt jelenti, hogy egy kibertámadó által megírt program az Internetet végigpásztázva próbálkozásokat tesz különböző rendszerek kihasználására. Ebből adódóan másodpercek alatt több ezer behatolási kísérletet is véghezvihető. Így a bűnözők képesek folyamatosan potenciális áldozatokat gyűjteni aránylag hatékony módon.

Az automatizált támadásokat végrehajtó botok listákból dolgoznak. Ezekbe beletartozik egyfelől a célpontok IP cím listája, azonban felhasználnak úgynevezett wordlisteket is, amelyek jelszó- és felhasználóneveket tartalmaznak. Ezek a listák gyakran illegális forrásokból származnak (főleg a darkweb piactereiről), amelyek valós internetfelhasználók belépési adatait tárolják, sokszor több száz millió soros méretben.



Az automatizált SSH támadások egyszerűsített topológiája

A jelszólisták közül talán a leghíresebb a „rockyou.txt" amely a RockYou vállalatott érintő 2009 támadáshoz vezethető vissza. Az incidens során a támadók SQL injection technikával több, mint 32 millió felhasználó érzékeny adatait (pédául e-mailcímeket és jelszavakat) nyertek ki a vállalati szerverekről, amelyeket nem sokkal utána közzétettek különböző platformokon. Habár az informatika világában 2009 viszonylag régnek tekinthető, az incidensből keletkezett jelszólista mai napig alapjául szolgál megannyi támadásnak.

A rockyou egy ma már publikusan is elérhető jelszólista, amely a hacker közösségekben és IT biztonsági szakértők körében nagy népszerűségnek örvendő Kali Linux operációsrendszer disztribúciókban „alapcsomagként" megtalálható.

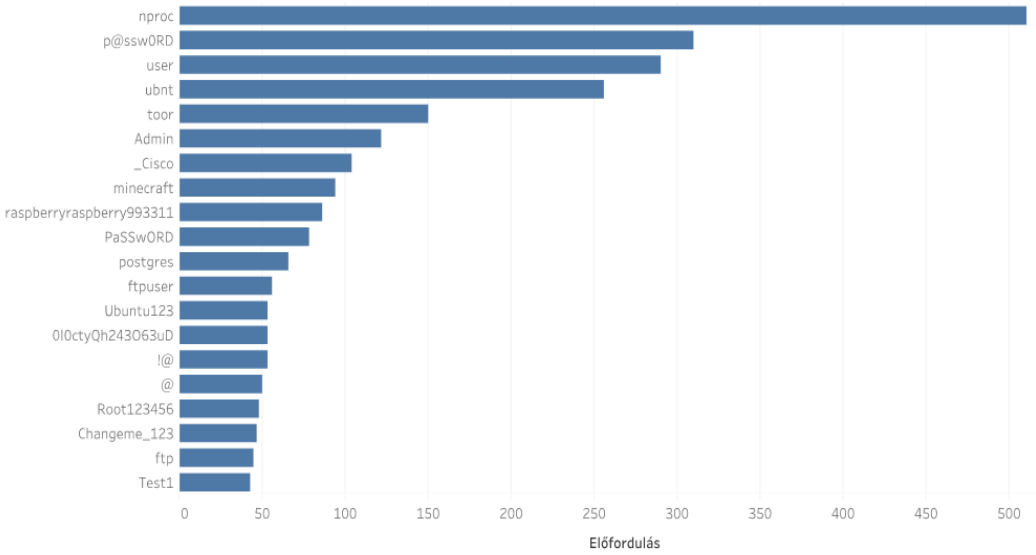
RockYou

Az vizsgált jelszavak erős kapcsolatot mutatnak a rockyou listával, a honeypotoknál felhasznált jelszavak 72,4%-a megtalálható ebben a jelszólistában. Ezekből ugyancsak az első három legnépszerűbb között végzett az *admin*, az *123456* és a *support* jelszavak, amelyek mind a gyenge jelszóválasztás tipikus példái. Mindezek mellett viszonylag gyakori a különböző számsorrendek és a *password* szó változatainak használata is.

Az érdekesség azonban a fennmaradó 28%-ban található, amely által észrevehető egyfajta generációs lépés az eredeti rockyou jelszólistához képest. Többek között feltűnőek a konkrét rendszerekre utaló szóösszetételek. Gyakoriak a Linux operációs rendszerekhez köthető szavak (mint például az *nproc* vagy az *Ubuntu*) de megtalálhatók még a Cisco routerekhez, Elastic és Ansible környezetekhez kapcsolható jelszavak is. A belépési kísérletekben és a jelszópróbálkozások választásában felfedezhető a Mirai és Mozi típusú malware robothálózatok (botnet) terjedései befolyása. Gyakori, hogy ezek a káros kódok sérülékeny routereket, és IoT eszközöket céloztak meg fertőzési kísérlettel.

Az említett malware trendekről bővebben olvashatnak a Nemzeti Kibervédelmi Intézet alábbi CTI jelentéseiben:

- A Mozi malware áttekintése
- IoT eszközök biztonsági kérdései – Az okosotthon
- IoT eszközök biztonsági kérdései – Az ipar

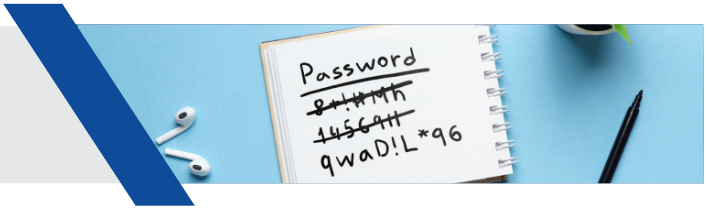


Top 20 jelszó, amely nem található meg a Rockyou listában

Javaslatok

Ebben a jelentésben prezentált felfedezések megmutatták a jelszavak kihasználására irányuló támadások körüli jellegzetességeket. **A könnyen kitalálható jelszavakkal védett rendszerek állandó célkeresztben állnak, használatuk pedig sokkal nagyobb kárt okozhat, mint azt elsőre gondolnánk.** Az automatizált támadások gigantikus mennyiségű fióktörési próbálkozást tesznek lehetővé, amely által könnyedén ajtót nyithatnak erőforrásainkhoz a kiberbűnözők számára. A következőkben néhány tanáccsal, jó gyakorlattal szeretnénk szolgálni, amelyek az előzőekben bemutatott támadási formákkal szemben megerősíthetjük rendszereink frontvonalbeli védelmét.

Tudatos jelszóhasználat



Jelszavaink legnagyobb gyengesége a jelszókezelésben rejlik. Rengeteg jelszót használunk, különféle platformokhoz és rendszerekhez, amely gyakran szinte átláthatatlanná válik. Már egyetlen erős jelszó megjegyzése is nehézségekbe ütközhet, azonban minden egyes felhasználói fiókunkhoz más-más belépési adatot már lehetetlen fejben tartani. Természetesen így a legkönnyebb azt választani, hogy mindenhova ugyanazt az egy, könnyen megjegyezhető jelszót használjuk. Ne essünk azonban a kényelem csapdájába, inkább alakítsunk ki egy jelszókezelési rendszert! Válasszunk egy számunkra szimpatikus jelszókezelő szoftvert, amelyben összegyűjtjük és folyamatosan aktualizáljuk az adatainkat! Ezáltal pontosan tisztában leszünk az összes hozzánk tartozó fiókkal, és nem kell időt töltenünk a jelszó kitalálásával, észben tartásával. Állítsunk be jelszavainknak élettartamot is! A hitelesítési adatok rendszeres lecserélése csökkenti a kompromitálódás esélyét. A legtöbb jelszókezelő már rendelkezik lejárati dátum beállításának lehetőségével, amely értesít minket, ha eljött az idő jelszócserére.

Multifaktoros hitelesítés (Multifactor Authentication - MFA)

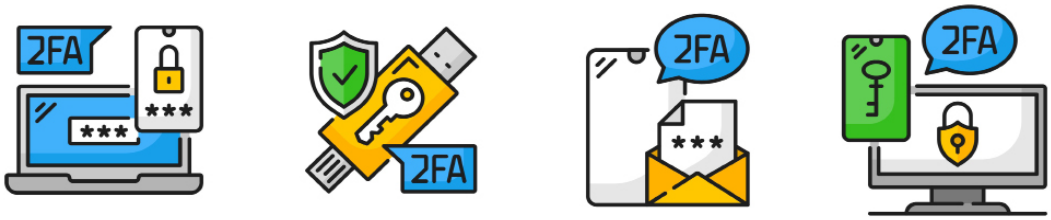
Amikor biztonságról beszélünk — legyen szó a fizikai világról vagy a kibertérről — akkor járunk el helyesen, ha nem elégszünk meg szimplán egyszintű védelemmel. **A multifaktoros hitelesítés lényege, hogy a megszokott felhasználónév-jelszó páros mellett egy harmadik — vagy ennél is több — hitelesítési lépésben biztosítjuk, hogy mi azok vagyunk, mint akinek mondjuk magunkat.** Ezáltal képesek vagyunk jelentősen csökkenteni annak az esélyét, hogy fiókunk kiberbűnözők által kompromittálódjon. Általában a tudásalapú felhasználónév és jelszó mellett másodiknak egy biometrikus, tanúsítványalapú, egyszerhasználatos jelkód vagy egy biztonsági kulcsos hitelesítést javasolt alkalmazni.

Az előző példához hasonlóan erősen ajánlott az SSH-t multifaktoros hitelesítéssel ellátni. Erre gyakori bevett választás a tanúsítványalapú hitelesítés, mint kiegészítés, azonban vannak megoldások, amelyek képesek alkalmazni egyszerhasználatos jelszavakat vagy hardveres tokeneket is.

SSH erősítés

A Secure Shell protokollt már hosszú idők óta egy igen hasznos és megbízható megoldásként tartjuk számon a rendszereink eléréséhez. Azonban az illetéktelen behatolók és kiberbűnözők — legyen az automatizáltan vagy személyesen — gyakorta próbára teszik az SSH-val ellátott rendszereink védelmét. Annak érdekében, hogy digitális erőforrásaink integritása megmaradjon, fontos alaposan átgondolnunk a védelmüket.

A kiberbűnözők csak azt a szolgáltatást képesek megtámadni, amire rálátásuk van. Ezáltal jó gyakorlat, ha az SSH-val felszerelt rendszereket a nyílt Internet felől nem tesszük elérhetővé, ehelyett VPN kapcsolat kiépítésével, egy védett hálózaton belül lehessen csak hozzáférni az SSH portokhoz. Ez a megoldás nemcsak elrejti a támadható felületeket, de extra titkosítást, és többlépcsős hitelesítést is képes nyújtani, ezzel jelentősen növelve rendszereink biztonságát.



NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2023