TLP:CLEAR
Szabadon terjeszthető!

Tájékoztató
Iráni kibercsoportok kritikus infrastruktúrát támadó tevékenységéről

(2024. október 18.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete tájékoztatót ad ki iráni kibercsoportok destruktív, a kritikus infrastruktúrát célzó támadásaival kapcsolatban, melyek során brute-force módszerrel és egyéb technikákat alkalmazva hajtanak végre támadó műveleteket. A műveletek célpontjai között szerepel többek között **az egészségügyi, a kormányzati és az energia szektor.** A támadók célja az áldozat hálózat hitelesítő adatainak megszerzése, amelyeket aztán kiberbűnözői fórumokon értékesítenek. A megvásárolt adatokat a bűnözők további rosszindulatú tevékenységek végrehajtására használhatják fel.

Az iráni csoportok ezirányú tevékenysége 2023 októbere óta megfigyelhető, támadási módszereik közé tartozik az MFA fiókok elleni password spraying, a brute-force támadás és az ún. „push-bombing" technika.

A tájékoztató több ügynökség (FBI, CISA, NSA, CSE, AFP) elemzése alapján készült, tartalmazza a támadó aktorok taktikáit, technikáit és eljárásait (TTP-k), valamint a kompromittáltsági mutatókat (IOC-k). Az információk az FBI-nak az e rosszindulatú tevékenység által érintett szervezetekkel folytatott megbeszéléseiből származnak.

A fent említett ügynökségek azt javasolják, hogy a kritikus infrastruktúrával foglalkozó szervezetek mindenképpen hajtsák végre az itt leírt mitigálási módszereket.

Technikai részletek:

A támadók valószínűleg felderítő műveleteket hajtanak végre az áldozatok személyazonosságára vonatkozó információk megszerzése érdekében. A hozzáférés megszerzése után a támadók különböző technikákat alkalmaznak további hitelesítő adatok szerzésére, a jogosultságok kiterjesztésére és a szervezet rendszereiről és hálózatáról szóló információk megszerzésére. A támadás során oldalirányú mozgás is megfigyelhető a feltört rendszerben, mely során további információkat töltenek le.

Kezdeti hozzáférés és perzisztencia:

A támadó csoportok érvényes felhasználói és csoportos e-mail fiókokat használnak, amelyeket brute-force támadással, például jelszószórással (password spraying) szereztek meg. Bizonyos esetekben ismeretlen módon szereztek hozzáférést Microsoft 365, Azure és Citrix rendszerekhez. Egyes esetekben, amikor a push értesítésen alapuló MFA (többfaktoros hitelesítés) engedélyezve volt, a támadók MFA kérelmeket küldtek a kérés elfogadását kérő legitim felhasználóknak. Ezt a technikát – a felhasználók bombázása mobiltelefon push értesítésekkel, amíg a felhasználó véletlenül jóvá nem hagyja a kérést, vagy leállítja az értesítéseket – „MFA fáradtságnak" vagy „push bombázásnak" nevezzük. Amint a támadók hozzáférnek egy fiókhoz, általában regisztrálják az eszközt többfaktoros hítelesítéssel, ezzel megvédve hozzáférésüket az adott környezethez.

A támadás során gyakran VPN-szolgáltatásokat használnak tevékenységeik elrejtésére, oldalirányú mozgáshoz pedig Remote Desktop Protocolt (RDP) alkalmaznak.

Detektálás

A brute-force tevékenység detektálásra, az ügynökségek javasolják a rendszer- és alkalmazásbejelentkezések hitelesítési naplóinak átnézését, különös tekintettel a sikertelen bejelentkezési kísérletekre vonatkozóan.

A virtuális infrastruktúrával kombinált, kompromittált hitelesítő adatok használatának észleléséhez a szerzői ügynökségek a következő lépéseket javasolják:

- Gyanús bejelentkezések változó felhasználónevekkel, karakterláncokkal és IP címkombinációkkal, vagy olyan bejelentkezések, amelyeknél az IP címek nem a felhasználó megszokott földrajzi helyéhez igazodnak.
- Több fiókhoz használt IP cím, kivéve a várható bejelentkezések.
- Lehetetlen utazás. Ha egy felhasználó több IP címről jelentkezik be, jelentős földrajzi távolsággal. Megjegyzés: Ennek az észlelési lehetőségnek a megvalósítása fals pozitív eredményeket hozhat, ha a felhasználók VPN-t alkalmaznak a hálózatokhoz való csatlakozás előtt.
- MFA regisztráció ismeretlen helyről vagy eszközökről.
- Olyan folyamatok és parancssori argumentumok, amelyek hitelesítő adatok dumpolására utalhatnak, különösen az ntds.dit fájl elérésére vagy másolására irányuló kísérleteket egy tartományvezérlőből.
- Gyanús fiókhasználat a jelszavak visszaállítása vagy a felhasználói fiókokkal kapcsolatos mitigációk alkalmazása után.
- Szokatlan tevékenységet a jellemzően inaktív fiókokban.
- Keresse a szokatlan, a normál felhasználói tevékenységhez jellemzően nem kapcsolódó stringeket, amelyek bottevékenységre utalhatnak.

Mitigáció:

Ezek az enyhítések összhangban vannak a CISA által kidolgozott, ágazatközi kiberbiztonsági teljesítménycélokkal (CPG-k), amelyek a Nemzeti Szabványügyi és Technológiai Intézet (NIST) Kiberbiztonsági Keretrendszeréhez igazodnak.

- IT Ügyfélszolgálat jelszókezelésének áttekintése, jelszóvisszaállítás zárolt fiókoknál és közös fiókoknál.
- Kerülje a gyakori jelszavakat (pl. „Spring2024” vagy „Password123!”).
- Tiltsa le a felhasználói fiókokat és a szervezeti erőforrásokhoz való hozzáférést a távozó alkalmazottak számára. A fiókok letiltásával minimálisra csökkenthető a rendszer kitettsége, és megszűnnek azok a lehetőségek, amelyeket a szereplők a rendszerbe való bejutáshoz kihasználhatnak. Hasonlóképpen, hozzon létre új felhasználói fiókokat a lehető legközelebb a munkavállaló munkába állásának időpontjához.
- Az adathalászat ellenálló MFA bevezetése.
- Folyamatosan vizsgálja felül az MFA beállításokat, hogy biztosítsa az összes aktív, internetre néző protokoll lefedettségét, hogy ne legyenek kihasználható szolgáltatások.
- Alapvető kiberbiztonsági képzés nyújtása a felhasználóknak, amely olyan fogalmakra terjed ki, mint például:
- Sikertelen bejelentkezési kísérletek észlelése.
- A felhasználóknak az általuk nem generált MFA kérelmek elutasítása.
- Annak biztosítása, hogy az MFA képes fiókokkal rendelkező felhasználók megfelelően állítsák be az MFA-t.

- A jelszóirányelvek összehangolása a legújabb NIST Digital Identity Guidelines (NIST digitális identitásra vonatkozó iránymutatások) szerint.
- A minimális jelszóerősség betartása.
- Az RC4 használatának kikapcsolása a Kerberos hitelesítéshez.

A szerzői ügynökségek azt is javasolják, hogy a szoftvergyártók építsék be a tervezési biztonság elveit és taktikáit a szoftverfejlesztési gyakorlatukba, hogy megvédjék ügyfeleiket a kompromittált hitelesítő adatokat használó szereplőkkel szemben, és ezáltal erősítsék ügyfeleik biztonsági helyzetét. A biztonságos tervezéssel kapcsolatos további információkért lásd a CISA Secure by Design weboldalát és közös útmutatóját.

IoC-k (Indicators of compromise):

Hash	**Leírás**
1F96D15B26416B2C7043EE7172357AF3AFBB002A	Rosszindulatú tevékenységhez kapcsolódik.
3D3CDF7CFC881678FEBCAFB26AE423FE5AA4EFEC	Rosszindulatú tevékenységhez kapcsolódik.

IP address	**Dátum**
95.181.234[.]12	01/30/2024 - 02/07/2024
95.181.234[.]25	01/30/2024 - 02/07/2024
173.239.232[.]20	10/06/2023 - 12/19/2023
172.98.71[.]191	10/15/2023 - 11/27/2023
102.129.235[.]127	10/21/2023 - 10/22/2023
188.126.94[.]60	10/22/2023 - 01/12/2024
149.40.50[.]45	10/26/2023
181.214.166[.]59	10/26/2023
212.102.39[.]212	10/26/2023
149.57.16[.]134	10/26/2023 - 10/27/2023
149.57.16[.]137	10/26/2023 - 10/27/2023
102.129.235[.]186	10/29/2023 - 11/08/2023
46.246.8[.]138	10/31/2023 - 01/26/2024
149.57.16[.]160	11/08/2023

149.57.16[.]37	11/08/2023
46.246.8[.]137	11/17/2023 - 01/25/2024
212.102.57[.]29	11/19/2023 - 01/17/2024
46.246.8[.]82	11/22/2023 - 01/28/2024
95.181.234[.]15	11/26/2023 - 02/07/2024
45.88.97[.]225	11/27/2023 - 02/11/2024
84.239.45[.]17	12/04/2023 - 12/07/2023
178.131.168[.]242	12/6/2023
46.246.8[.]62	12/6/2023
212.102.57[.]214	12/6/2023
179.61.228[.]35	12/6/2023
46.246.41[.]165	12/6/2023
154.16.192[.]104	12/6/2023
46.246.8[.]104	12/07/2023 - 02/07/2024
37.46.113[.]206	12/07/2023
46.246.3[.]186	12/07/2023 - 12/09/2023
46.246.8[.]141	12/07/2023 - 02/10/2024
46.246.8[.]17	12/09/2023 - 01/09/2024
37.19.197[.]182	12/15/2023
154.16.192[.]38	12/25/2023 - 01/24/2024
102.165.16[.]127	12/27/2023 - 01/28/2024
46.246.8[.]47	12/29/2023 - 01/29/2024
46.246.3[.]225	12/30/2023 - 02/06/2024
46.246.3[.]226	12/31/2023 - 02/03/2024
46.246.3[.]240	12/31/2023 - 02/06/2024
191.101.217[.]10	01/05/2024
102.129.153[.]182	01/08/2024
46.246.3[.]196	01/08/2024

102.129.152[.]60	01/09/2024
156.146.60[.]74	01/10/2024
191.96.227[.]113	01/10/2024
191.96.227[.]122	01/10/2024
181.214.166[.]132	01/11/2024
188.126.94[.]57	01/11/2024 - 01/13/2024
154.6.13[.]144	01/13/2024 - 01/24/2024
154.6.13[.]151	01/13/2024 - 01/28/2024
188.126.94[.]166	01/15/2024
89.149.38[.]204	01/18/2024
46.246.8[.]67	01/20/2024
46.246.8[.]53	01/22/2024
154.16.192[.]37	01/24/2024
191.96.150[.]14	01/24/2024
191.96.150[.]96	01/24/2024
46.246.8[.]10	01/24/2024
84.239.25[.]13	01/24/2024
154.6.13[.]139	01/26/2024
191.96.106[.]33	01/26/2024
191.96.227[.]159	01/26/2024
149.57.16[.]150	01/27/2024
191.96.150[.]21	01/27/2024
46.246.8[.]84	01/27/2024
95.181.235[.]8	01/27/2024
191.96.227[.]102	01/27/2024 - 01/28/2024
46.246.122[.]185	01/28/2024
146.70.102[.]3	01/29/2024 - 01/30/2024
46.246.3[.]233	01/30/2024 - 02/15/2024

46.246.3[.]239	01/30/2024 - 02/15/2024
188.126.89[.]35	02/03/2024
46.246.3[.]223	02/03/2024
46.246.3[.]245	02/05/2024 - 02/06/2024
191.96.150[.]50	02/09/2024

Device type	**Leírás**
Samsung Galaxy A71 (SM-A715F)	MFA regisztrált
Samsung SM-G998B	MFA regisztrált
Samsung SM-M205F	MFA regisztrált

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu