APT-42

Az APT42, egy iráni állam által támogatott számítógépes kémcsoport, amely az iráni kormány stratégiai érdeklődési körébe tartozó egyének és szervezetek ellen indított információgyűjtési és megfigyelési műveleteket. Sejthető, hogy az APT42 az Iszlám Forradalmi Gárda Hírszerző Szervezetének (IRGC-IO) megbízásából működik, olyan célpontokat megtámadva, amelyek az szervezet operatív feladatkörébe és prioritásaihoz illeszkednek. APT42 Műveletek: Az APT42 erősen célzott szigonyozás (spear-phishing) és social engineering technikákat használ, amelyek célja a bizalom és kapcsolat felépítése az áldozataival annak érdekében, hogy hozzáférjen személyes vagy vállalati e-mail fiókjaihoz, vagy Android malware-t telepítsen mobil eszközeikre. Emellett az APT42 időnként Windows malware-t is használ a hitelesítő adatok gyűjtéséhez és megfigyeléseik kiegészítésére. Az APT42 műveletek három kategóriába sorolhatók:

Hitelesítő adatok gyűjtése: Az APT42 gyakran célzott vállalati és személyes e-mail fiókokat személyre szabott kampányokkal, amelyek erős hangsúlyt fektetnek a bizalom és a kapcsolat kialakítására a célponttal, mielőtt megpróbálják ellopni hitelesítő adataikat. Megfigyelési műveletek: Legalább 2015 végéig az APT42 infrastruktúrájának egy része parancs- és vezérlő (C2) szerverként szolgált Android mobil malware-hez, amelyet általában az iráni kormány számára érdekes egyének tevékenységének megfigyeléséhez használtak. Malware telepítése: Habár az APT42 elsősorban a hitelesítő adatok gyűjtését részesíti előnyben a merevlemezen végrehajtott tevékenységgel szemben, több saját backdoort és egyszerűbb eszközt is alkalmaznak. A csoport valószínűleg ezeket is beépíti műveleteibe, amikor a célok túlmutatnak a hitelesítő adatok gyűjtésén. Az APT42 műveleteinek célzás mintái hasonlóak más iráni számítógépes kémcsoportokhoz, azonban eltérően más feltételezett IRGC-hoz köthető ilyen csoportoktól, az APT42 főként azokat a szervezeteket és személyeket célozza meg, amelyek az iráni rezsim ellenfelei vagy ellenségei, konkrétan hozzáférést szerezve személyes fiókokhoz és mobil eszközökhöz. A csoport folyamatosan célba veszi a nyugati intézeteket, kutatókat, újságírókat, jelenlegi nyugati kormánytisztviselőket, korábbi iráni kormánytisztviselőket és az iráni diaszpórát külföldön. Az APT42 tevékenységéből kiderül, hogy a csoport megváltoztatja műveleti fókuszát, ahogy Irán prioritásai változnak, ideértve a COVID-19 járvány kezdetén, 2020 márciusában a gyógyszeripari szektor, valamint a belföldi és külföldi ellenzéki csoportok ellen irányuló céltudatos műveleteket egy iráni elnökválasztás előtt. Nem várunk jelentős változásokat az APT42 operatív taktikáiban és feladatkörében, figyelembe véve a hosszú történelmet és az infrastruktúra lebontásával és az operatív biztonsági hibák nyilvánosságával szembeni ellenálló képességet. Mindazonáltal a csoport képességét már bebizonyította arra, hogy gyorsan megváltoztatja operatív fókuszát, ahogy az iráni prioritások az idővel változnak az ország bel- és geopolitikai feltételeinek változásával összhangban. Magas bizalommal értékeljük, hogy az APT42 továbbra is kibervédelmi és megfigyelési műveleteket fog végrehajtani, az iráni műveleti hírszerzési gyűjtési követelményekkel összhangban.