Tomori Levente

APT-42

2023

A 42-es számú APT (Advanced Persistent Tthreat) csoport tevékenységének rövid összefoglalója

www.nki.gov.hu

tomorilevente@gmail.com

APT-42

Irán

Az APT-42, 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 APT-42 az Iszlám Forradalmi Gárda Hírszerző Szervezetének (IRGC-IO) megbízásából működik, olyan célpontokat megtámadva, amelyek a szervezet operatív feladatkörébe és prioritásaihoz illeszkednek.

Az APT-42 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 APT-42 időnként Windows malware-t is használ a hitelesítő adatok gyűjtéséhez és megfigyeléseik kiegészítésére.

Az APT42 műveletek három kategóriába sorolhatók:

1. Hitelesítő adatok gyűjtése:

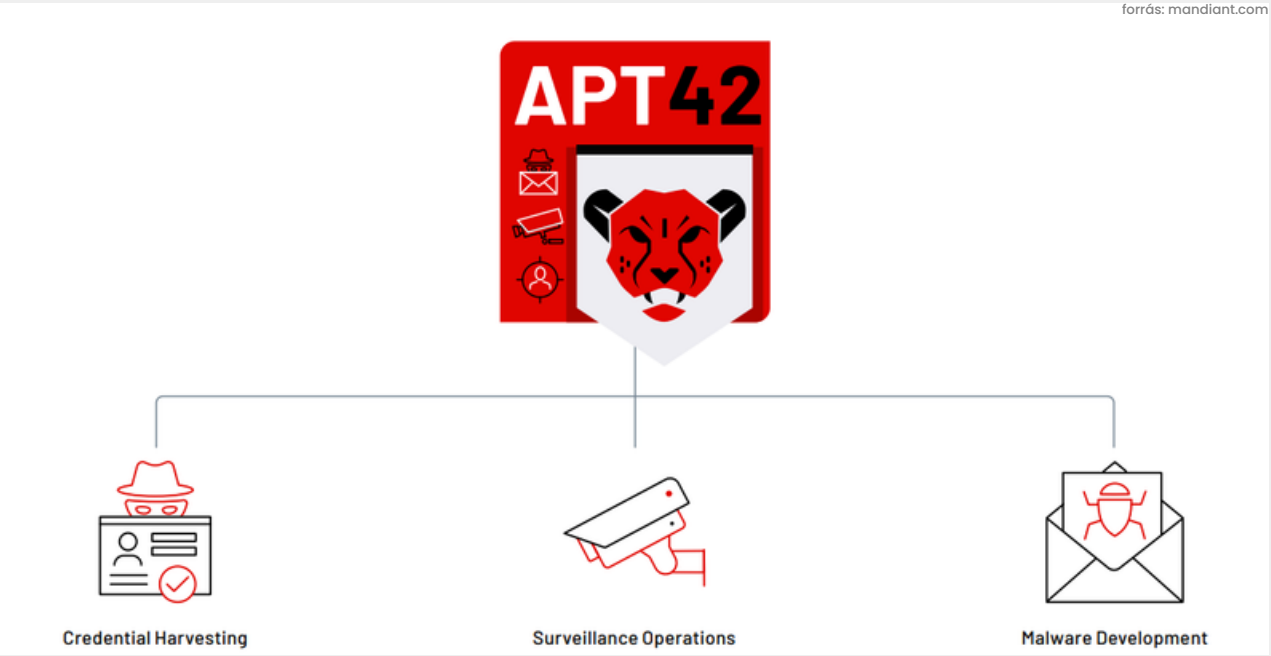
Az APT-42 gyakran célzott vállalati és személyes e-mail fiókokat személyre szabott kampányokkal, amelyek erős hangsúlyt fektetnek a bizalom és a kapcsolat kialakítására a célponttal, mielőtt megpróbálják ellopni hitelesítő adataikat.

2. Megfigyelési műveletek:

Legalább 2015 végéig az APT-42 infrastruktúrájának egy része parancs- és vezérlő (C2) szerverként szolgált egy Android mobil malware-hez, amelyet általában az iráni kormány számára érdekes egyének tevékenységének megfigyeléséhez használtak.

3. Malware telepítése:

Habár az APT-42 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 APT-42 célzásmintái

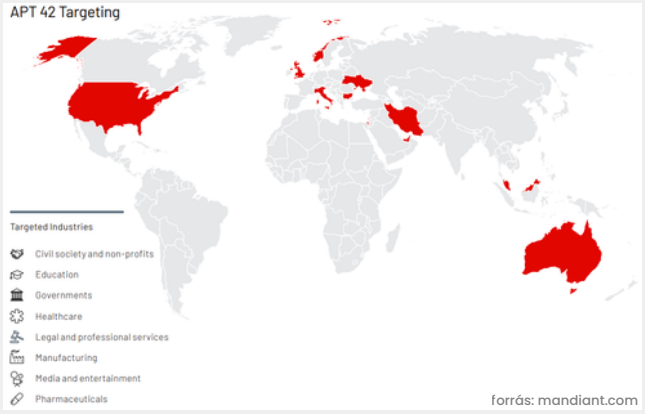
Az APT-42 műveleteinek célzás mintái hasonlóak más iráni számítógépes kémcsoportokhoz, azonban eltérően más feltételezett IRGC-hoz köthető ilyen csoportoktól, az APT-42 főként azokat a szervezeteket és személyeket célozza meg, amelyek az iráni rezsim ellenfelei vagy ellenségei, konkrétan hozzáférést szerezve személyes fiókokhoz és mobil eszközökhöz.

A csoport folyamatosan támadja a nyugati intézeteket, kutatókat, újságírókat, jelenlegi nyugati kormánytisztviselőket, korábbi iráni kormánytisztviselőket és az iráni diaszpórát külföldön.

Az APT-42 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 az iráni elnökválasztás előtt.

Az APT-42 által célzott országok és iparágak

Az APT-42 tevékenységének 2015-ös első megfigyelése óta legalább 14 ország szervezeteit célozta meg beleértve Ausztráliát,
Európát, a Közel-Keletet és az Egyesült Államokat.



Az APT42 a következő ágazatokat célozta meg:

- Civil társadalmi és nonprofit szervezetek
- Oktatás
- Kormányzatok
- Egészségügy
- Jogi és szakmai szolgáltatások
- Gyártás
- Média és szórakoztatás
- Gyógyszeripar

Előretekintés

Nem várható jelentős változás az APT-42 operatív taktikáiban és feladatkörében, figyelembe véve az infrastruktúrájukra mért csapásokkal és az operatív biztonsági hibáik nyilvánosságra hozatalával szembeni ellenálló képességet.

Mindazonáltal a csoport azt a képességét már bizonyította, hogy gyorsan megváltoztatja operatív fókuszát, ahogy az iráni prioritások az idővel változnak az ország bel- és geopolitikai feltételeinek változásával összhangban.

Több, mint valószínű, hogy az APT-42 továbbra is támadásokat és megfigyelési műveleteket fog végrehajtani, az iráni műveleti hírszerzési követelményekkel összhangban.