CTI Jelentés

# A Mozi malware áttekintése

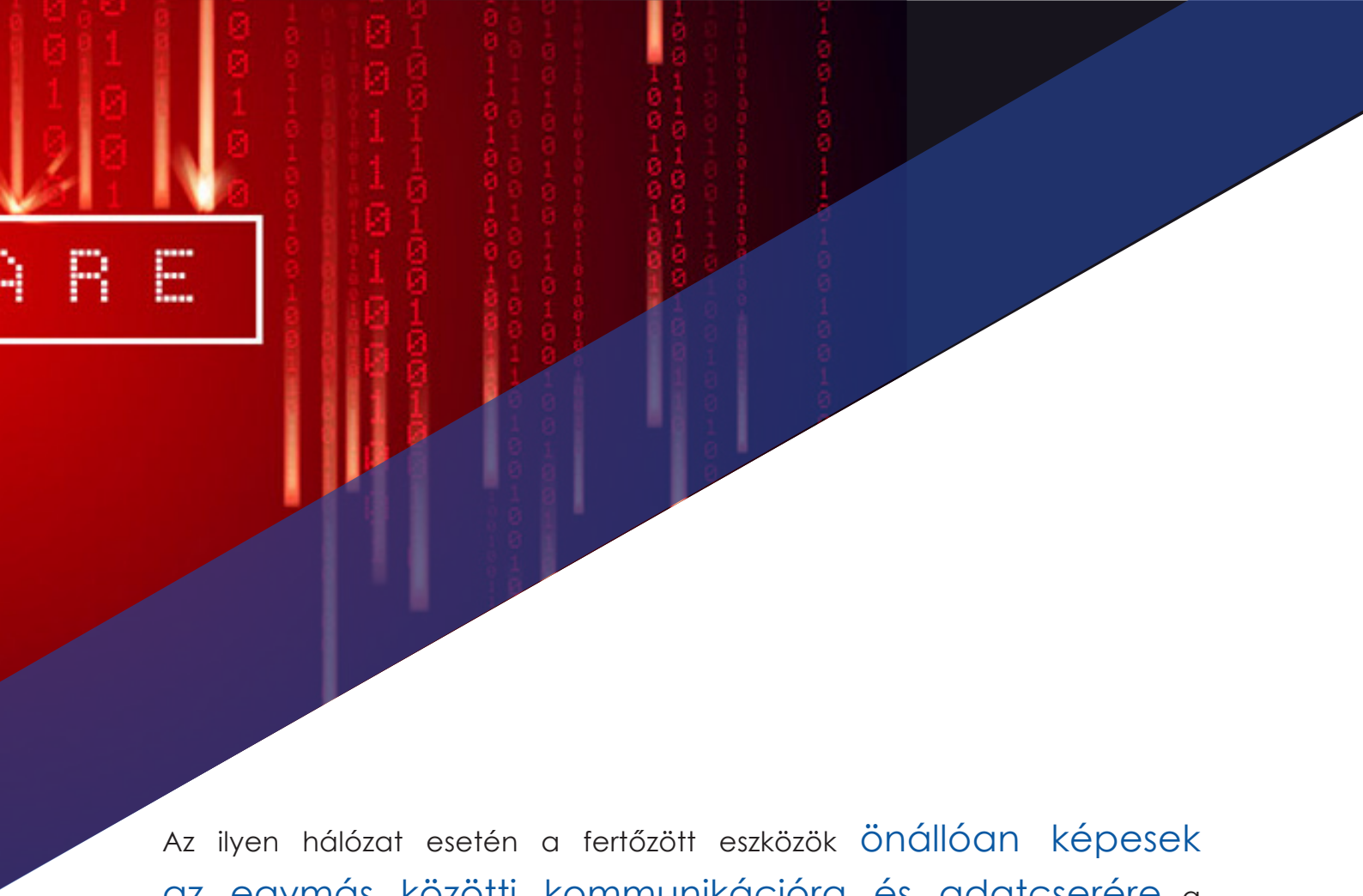
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET


# Bevezetés

A Mozi egy Peer-To-Peer (P2P) kapcsolat alapú botnet káros kód, amely elosztott hash táblákat (DHT – Distributed Hash Table) használ fel a kommunikáció során. Sok hasonlóságot mutat a már korábban felbukkant Gafgyt, IoT Reaper és Mirai malware karakterisztikáival.

Hasonlóan a nagy népszerűségnek örvendő Torrent hálózatokhoz, a Mozi malware is elosztott hash táblák segítségével alakítja ki a P2P felépítést. Ennek segítségével lehetőség nyílik a központi koordinátort, mint például egy centralizált irányító szervert vagy más néven C2 szervert teljesen mellőzni.



Az ilyen hálózat esetén a fertőzött eszközök önállóan képesek az egymás közötti kommunikációra és adatcserére a frissítések érdekében. Ezek megszüntetése igen nehéz, mivel ehhez az összes csomópontot meg kellene szüntetni. A P2P hálózatok esetén szükséges az összes fertőzött gép kiiktatása, mivel egyetlen „túlélő" esetén is képes aktívan működni és terjeszkedni. Az ilyen P2P jellegű hálózat kiépítés nagy előnye még, hogy a megosztott hálózati forgalom miatt nehezen válik észlelhetővé a botnet kommunikációra jellemző hálózati abnormalitás.

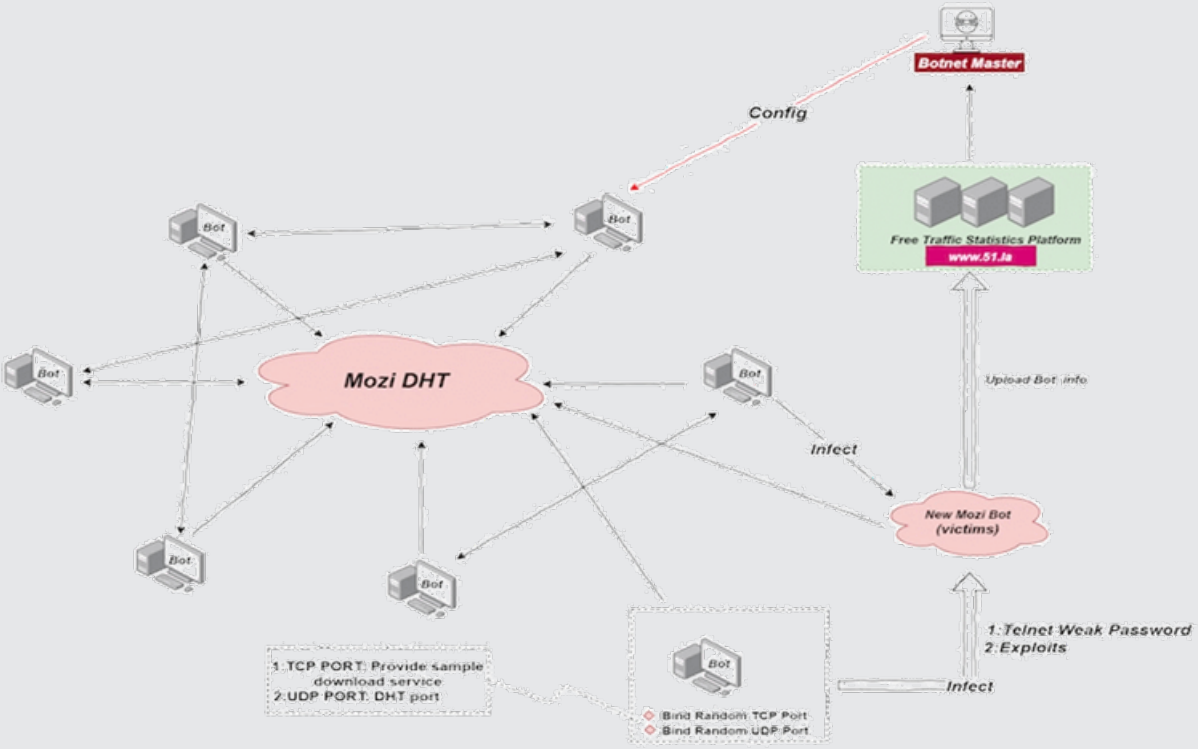
A fertőzött eszköz és a hálózaton található összes csomópont egységesen és külön-külön is az alábbi tevékenységeket képes elvégezni:

- DDoS támadás
- Kriptobányászat
- Közbeékelődéses támadás fertőzött routerek esetében
- Bot információk lekérdezése
- A fertőzött eszközön található malware frissítése
- Egy specifikus URL-en található programsorok lefuttatása
- Parancsok végrehajtása

# A történelmi ős-malware: Mirai

A 2016-os évben egy, addig még ismeretlen típusú malware által megfertőzött, IoT eszközökből álló botnet hálózat hívta fel magára a figyelmet, amely később a kártevő elnevezése után a Mirai nevet kapta. A malware fertőzésekből kiépített botnet hálózat DDoS támadásokkal vonta magára a figyelmet, amelynek ereje elérheti a masszív 1 Tbps hálózati sávszélességet. Az áldozatok között szerepelt például a Dyn egyesült államokbeli DNS szolgáltató, a francia OVH szolgáltató és a Deutsche Telekom is. Miután a GitHub közösségi szoftver-verziókövetéssel foglalkozó oldalon megosztották a forráskódját, több, hasonló elven működő kártevőben felhasználták részben vagy egészben a scriptet.

A Mirai kódján alapuló Mozi malware először 2019 decemberében került a kutatók látókörébe, amikor egy másik, hasonló malware kapcsán nem várt hálózati forgalomnövekedést regisztráltak. A Black Lotus Lab kutatói az IoT Reaper nevű kártevőhöz kapcsolták az eseményeket, azonban hamar kiderült, hogy annak egy új, gyorsan terjeszkedő variánsával állnak szemben.




A Mozi botnet sematikus felépítése és vázlatos működési ábrája

## Terjedés

A kimondottan gyors terjedés a kártevő felépítésének köszönhető. A rendszerek hozzáféréséhez két metódus típust tudunk megkülönböztetni a Mozi malware esetében.

Egyfelől rendszergazdai hozzáférést képes szerezni a legyakoribb, egyszerű és gyenge jelszavak végig próbálásával. Sok esetben a routerek és egyéb IoT eszközökhöz tartozó admin felhasználói fiókok a gyárilag beállított, interneten megtalálható jelszavaival rendelkeznek.

Másik bevett lehetőség a megfelelő jogosultsági szint eléréséhez az eszközök sérülékenységének kihasználása.

A behatoláshoz először a támadó fél egy véletlenszerű porton generált http kéréssel tesz próbát sérülékenységek kihasználására, amellyel rendszergazdai jogosultságot szerezhetnek. A http kérés valójában egy rejtett parancs (CMDi - command injection), amely kísérletet tesz a számítógépen található rendszermappába írásra. Ha ez a kísérlet sikerrel járt, a parancs által írt fájl (Mozi.a vagy Mozi.m) lefuttatásra kerül, és letölti a kártevőt tartalmazó, az eszköz architektúrájához illeszkedő fájlokat. Amennyiben ez a módszer nem jár sikerrel, a kártevő megpróbál az interneten publikusan elérhető alapértelmezett felhasználónév/jelszó párosok segítségével belépni az eszközre és elvégezni ugyanezeket a lépéseket.

| VULNERABILITY | AFFECTED AEVICE |
|---|---|
| Eir D1000 Wireless Router RCI | Eir D1000 Router |
| Vacron NVR RCE | Vacron NVR devices |
| CVE-2014-8361<br><br>Netgear cig-bin Command Injection | Devices using the Realtek SDK<br><br>Netgear R7000 and R6400 |
| Netgear setup.cgi unauthenticated RCE<br><br>JAWS Webserver unauthenticated shell command execution | DGN1000 Netgear routers<br><br>MVPower DVR |
| CVE-2017-17215 | Huawei Router HG532 |
| HNAP SoapAction-Header Command Execution<br><br>CVE-2018-10561, CVE-2018-10562 | D-Link Devices<br><br>GPON Routers |
| UPnP SOAP TelnetD Command Execution<br><br>CCTV/DVR Remote Code Execution | D-Link Devices<br><br>CCTV DVR |

A Mozi kártevő kódjában eddig felfedezett sérülékenységek és kapcsolódó eszközök

A fájlok letöltését követően a kártevő megkezdi működését a fertőzött eszközön. Lefoglalja a 14373-as UDP portot saját felhasználásra. Emellett az összes 1536-os és 5888-as portot használni kívánó alkalmazás futását megszünteti (pkill paranccsal). Az utóbbi tevékenységet feltehetőleg a többi botnet fertőzés elkerülésére teszi, amelyek ugyanúgy kihasználhatják az eszköz sérülékenységeit.

Annak érdekében, hogy a fertőzött eszköz a többi csomóponttal képes legyen kommunikációt lefolytatni és parancsokat fogadni, legenerálódik egy 20 bájt hosszúságú egyedi azonosító. Az ID létrehozása után regisztrálja magát a káros kódba égetett 8db csomópontnál a DHT protokoll alapján. A sikeres regisztrációt követően visszajelzésként egy titkosított konfigurációs állományt kap vissza a csomóponttól, ami tartalmazza az ismert csomópontok listáját és a fertőzött eszköz szerepkörét is. A szerepkörök közül eddig „bot", „sk", „ftp", „sns" elnevezéseket figyeltek meg.

Az ismert csomópontok listájának segítségével egyrészt elkerüli az újra fertőződést és ezáltal a már aktív malware felülírását, másrészt frissítéseket és utasításokat kaphat az elosztott hálózatról.

Érdekessége a Mozi malwarenek, hogy tudatos lépést tesz a más, nem megbízható fél által kiadott parancsok és üzenetek védelme ellen. Integritásának megőrzése érdekében ECDSA 384-es algoritmust használ fel a beérkező fájlok és üzenetek legitimálására, amelyet 2 darab XOR publikus kulccsal képes ellenőrizni.

Jellemző még rá, hogy a fertőzést elindító fájl (dropper) nem, azonban a tényleges malware-t tartalmazó fájlok már egyedileg, az adott eszköz operációs rendszerére szabottan kerülnek elkészítésére (UPX packing). Ez az algoritmus hasonlóan más malwarekhez védelmet nyújt a káros kód észlelésének elkerülése érdekében.

## Jelentősége:

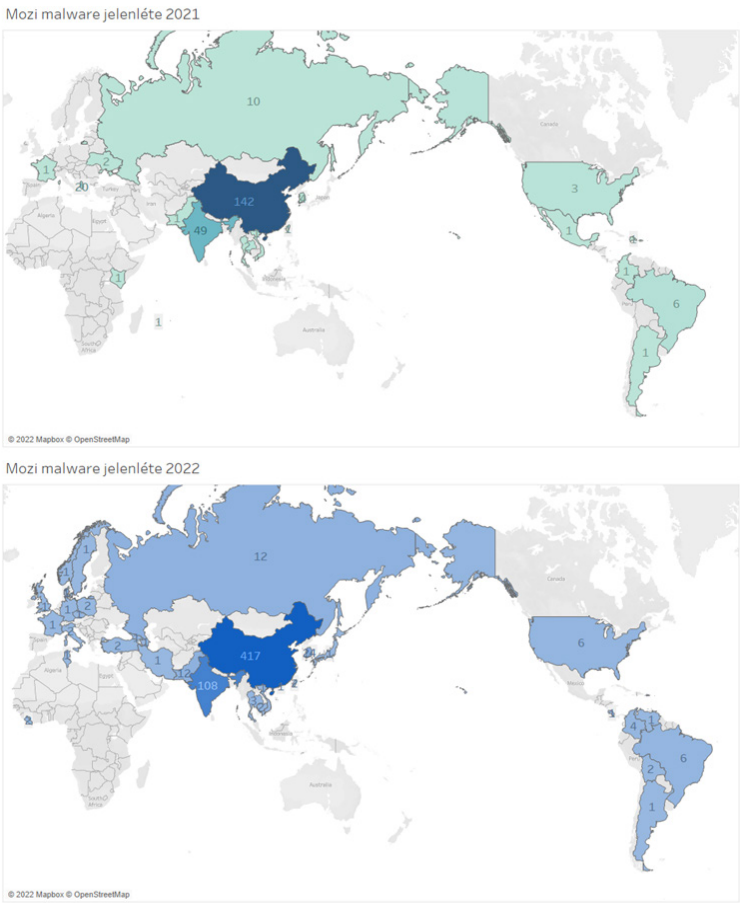
Köszönhetően a botnet elosztott (P2P) hálózati jellegének, a kártevő nehezen felfedezhető. Az IBM X-Force megfigyelései alapján ez igen jelentős, 400%-os növekedést okozott az IoT eszközökről érkező támadások területén a 2019 harmadik negyedévétől 2020 második negyedévéig terjedő időszakban. Ezen forgalomnak a 90%-a volt valamilyen módon köthető a Mozi botnet tevékenységéhez.

A dél-koreai titkosszolgálat, a National Intelligence Service (NIS) – az orosz hatóságokkal végzett közös munka során – 2021 decemberében fedezett fel körülbelül 12.000 Mozi malware-rel fertőzött IoT eszközt 72 különböző országban. Ezen készülékek többsége CCTV kamerákat, otthoni routereket, és digitális videó rögzítőket (DVR) foglal magába.

## Az NKI statisztikái

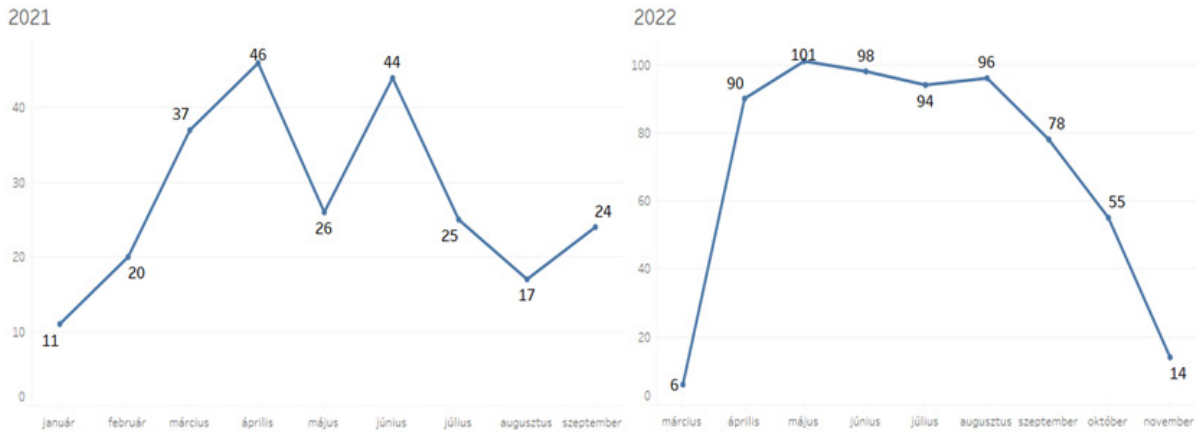
A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Honeypot rendszere évek óta nyújt friss adatokat a kibertér állapotáról. A Mozi malware folyamatos nyomonkövetése után megállapítható pár érdekesség.

A Mozi 2022-ben az 5 legnagyobb számú eseménnyel rendelkező malware típusok között található. Heti rendszerességgel körülbelül 19 esemény csatolható ezen káros kódhoz különböző forrásokból. A Mozi hálózat kiterjedtségét mutatja, hogy minden esemény különböző forrás IP címről érkezett a csapdarendszerek felé, amelyek jelenleg 621 különböző eszközre utalnak. Országokra bontva erős ázsiai dominanciát láthatunk, mivel a legtöbb eseményszám forrásai elsősorban Kína, India, Dél-Korea, Oroszország és Pakisztán. Ezenkívül érdemes még megfigyelni a fertőző eszközök terjedését az alábbi ábrán. Az események mértékének növekedése mellett nagyobb területi térhódítás fedezhető fel, amely több európai és ázsiai országot érint.




A GovProbe csapdarendszerekbe befutó Mozi malwarek eloszlása forrásország szerint

Az utóbbi két évben felfedezhető több érdekesség. Az alábbi ábrán látható ahogy 2021 szeptemberétől megszakad a regisztrált események folyamata. Az egyébként egyenletes mértékkel változó számok teljes megszűnése annak köszönhető, hogy abban az időben a kínai rendfenntartó erők elfogták a Mozi malware készítőit és kiiktatták a hozzájuk kapcsolható szolgáltatásokat, azonban 6 hónap elteltével márciusban (ugyan még kis számban) visszatért a Mozi malware. Kezdetben havi 6 Mozi tevékenységhez köthető eseményszám áprilisra meghaladta a 90-et, amely a 2021-es év átlagának több, mint duplájáját jelentette.




Mozi malware beérkező eseményeinek változása a 2021-22 években

# A támadási láncolat:

A Microsoft 2021 augusztusában publikált jelentése megpróbálja felhívni a figyelmet a Mozi malware veszélyforrásaira és az ellene tehető proaktív védekezésre. A jelentés tartalmazza a támadási láncolat (kill chain) és folyamatok részletezését a hálózati eszközök megfertőzésével kapcsolatban.

1. Az internet feltérképezése: Első lépésként (amely az más malwarekre is jellemző) a támadó különböző scan megoldásokkal (pl.: Shodan) felkutatja a sérülékeny célpontokat.

2. Célpontok felderítése: A támadó az internet átjáró irányából felderíti a kiválasztott célpontot. Szükség esetén további scanneket alkalmaz.

3. Sérülékenység kihasználása: A már előzőleg felderített sérülékenységek ismeretében kisebb utánajárással könnyedén beszerezhető azok kihasználására tervezett módszer vagy káros kód. Amennyiben ez sikertelennek bizonyul úgy a gyenge jelszavakat tartalmazó szólista alapú brute force módszerrel tehet próbát a támadó.

4. Mozi telepítése: A támadó telepíti és megfertőzi a hálózati átjárót a Mozi malwerrel.

5. Jelenlét kiépítése: A káros kód ezen szakaszban egy scriptet futtat le a megfertőzött eszközön, amely segítségével egy esetleges újraindítás után is ki tudja építeni a kapcsolatot a C2-es irányítószerver és a kliens között vagy a P2P csomópontokkal.

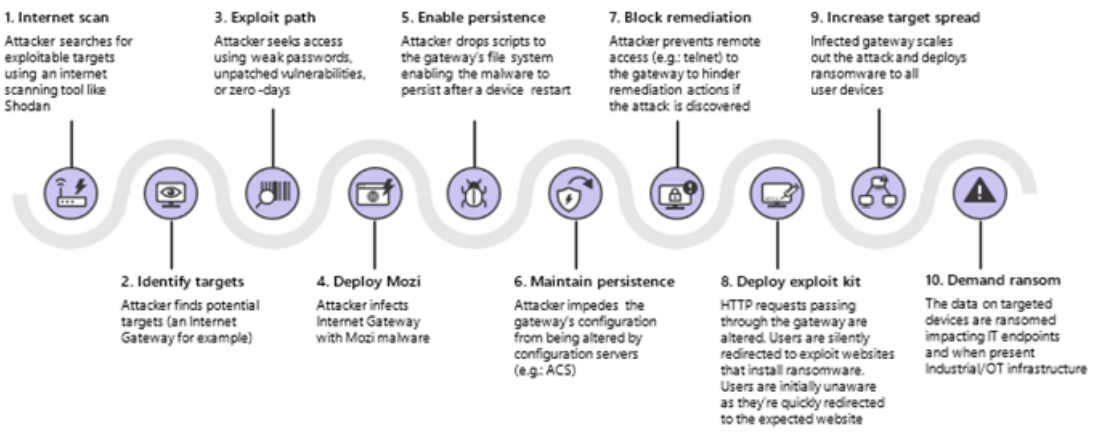
6. Jelenlét fenntartása: Konfigurációk változtatása az adott hálózati átjáróra jellemző sérülékenységek kihasználásával, amely által egy automatikus konfigurációs szerver (ACS) sem képes a kapcsolat felbontására vagy változtatására.

7. Helyreállítás akadályozása: A támadó letiltja a távoli hozzáféréshez fenntartott szolgáltatásokat és a hozzátartozó portokat. Ezáltal megakadályozza, hogy a rendszergazdák ilyen módon képesek legyenek az eszköz visszaállítására és a támadás megszüntetésére.

8. Exploit kit telepítése: A hálózati átjárón minden látható forgalom áthalad. A közbeékelődött támadó így a nem titkosított http üzeneteket könnyedén módosítani tudja. Ezáltal az áldozat kérése a tudta nélkül, feltűnésmentesen átirányításra kerülhet egy ransomware-t tartalmazó weboldalra.

9. A fertőzés terjedésének felgyorsulása: A script ezután minden hálózaton látható eszközre továbbítja a káros kódot, kiszélesítve a fertőzött eszközök számát. Ez a folyamat exponenciális gyorsaságban is lefolyhat.

10. Váltságdíj követelése: A sikeres tömeges fertőzés után a támadó az áldozat tudtára adja a követeléseit az adatok feloldásért cserébe.




Mozi attack kill chain - kép forrása

# Védekezés a Mozi malware ellen:

A malware fertőzésének kockázatát a támadási felület csökkentésével tudjuk elérni. A Mozi esetében ez a sérülékenységek kihasználásának vagy jogosultságok megszerzésének megakadályozását jelenti.

Először is fontos, hogy az eszközeinkhez használt belépési hitelesítő adatok legyenek erősek, és változtassuk őket rendszeresen. Ezáltal meg tudjuk előzni, hogy a támadást kiszivárgott jelszó listákkal vigyék sikerre. Eszközeink mindig legyenek napra készek! A vállalatok által kiadott firmware frissítések funkciójavítás mellett fontos biztonsági foltozásokat is tartalmazhatnak. Mindig kövessük figyelemmel ez elérhető frissítéseket vagy amennyiben elérhető, állítsuk be a frissítések automatikus telepítését!

NEMZETI
KIBERVÉDELMI INTÉZET


nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast


2022