Xiongmai sztori

Szeretjük a modern kütyüket, ezek fontos fokmérői, hogy hogyan viszonyulunk a technológiai fejlődéshez, azaz mennyire vagyunk menők. Bevallom, ebből a szempontból egyáltalán nem (sem) vagyok menő.

Sógorom, Kori, aki nagy mobil-guru, mindig körberöhög a nem túlzottan leplezett paranoiámmal ezzel a modern világgal szemben.

Pedig ismerem az egésznek a hátterét, az átviteli protokollokat, a jelszinteket és hogy mitől működik az egész; talán éppen ez az ismeret tesz meglehetősen kétkedővé.

Gond nélkül megvesszük a hangvezérléses asszisztenst, a lakást felügyelő kamerákat és az önszántából árut rendelő szuper kütyüket, aztán meg csodálkozunk. Csodálkozunk, hogy az este az asszonynak privát show keretei között bemutatott *helikopterezés* (hungarikum!) egy héttel később a *napiszaron* köszön vissza ránk (szintén hungarikum!).

Persze ilyenkor elgondolkodunk a miérteken, miközben a kamera földi maradványaival megcélozzuk a ház előtti utcán, özvegy Kovácsné mellett éppen a járdára kitárazó tartályforma Bizsu kutyát.

Fel sem tűnik, hogy a nagy modernizálás varázsával eltelve teljesen megfeledkezünk az alapvető biztonsági lépésekről, például hogy megnézzük, hogy honnan is származik a csili-vilire pimpelt kamera. Ha van még egy kis türelme, elmondom.

Ja igen, mielőtt belevágnék ebbe a történetbe, egy újítást szeretnék bemutatni a blogon. Az írásaimmal mindig próbálok egyensúlyozni a közérthetőség és a technikai hitelesség között. Nyilván, ha ez utóbbira koncentrálnék, a legtöbb olvasom simán bealudna, ezért azt találtam ki, hogy a szintén általam írt OB121 oldalra átvezető linkeket fűzök be a bejegyzésekbe, például így: IoT. Ott – remélem – a megoldások technikai hátterét is kielégítő módon tudom majd tisztázni.

Jó 10-20 éve alapították meg a távol-keleten – Kínában, Fülöp-szigeteken, Thailandon,.. – az első dzsunkacégeket. Ezek eleinte bér-összeszereléssel foglalkoztak, közvetlenül a halpucoló és cápákat uszonytalanító munkások mellett olyan alkatrészeket szereltek össze, amire már a fényes nyugaton senki nem volt hajlandó. Jórészt ezekből a cég-kezdeményekből alakultak ki a mai milliós-milliárdos

forgalmú, gyakorlatilag rabszolgasorba kényszerített munkásokkal dolgoztató hatalmas, de többnyire ismeretlen cégek.

Sokat elárul az itteni munkahelyekről az un. **Foxconn-háló**; a cég a gyártócsarnokaira hálót szereltetett, hogy megakadályozza, hogy a melósai ott öngyilkosok legyenek. Menjenek csak haza, és oldják meg otthon, illetve hát a tömegszállásokon a magánéleti problémáikat.

A hirhedt Foxconn-hálók egyike. A névadó nem biztos, hogy büszke rá..

Az itt eszméletlen mennyiségben legyártott készüléket aztán konténerekben behajózzák, hogy egy hónapnyi utazás után Rotterdamban vagy Hamburgban kirakodhassák. Nem, ezek így még többnyire nem kerülnek forgalomba, gondos török, pakisztáni vagy szomáliai munkáskezek szakavatott mozdulatokkal átcímkézik és átcsomagolják először ezeket, csak hogy sokszoros áron és hívogató dobozokban kerülhessenek a kereskedelmi óriáscégek polcaira.

Otthon a kicsomagolt IoT kameráknak IoT automatikusan engedélyezzük a net-elérést, azok automatikusan csatlakoznak is a felhőjükhöz, és kész. Gondolhatnánk.

Xiongmai

Egy ilyen cég a címadó **Xiongmai** is; a nevét senki nem ismeri, de komoly esélye van, hogy valamelyik itt gyártott kütyü valahol ott bújik meg az ön asztalán is. Ugyanis a Xiongmai helyett több, mint 100 egyéb márkanéven kerülnek ezek forgalomba (ezeknek a neveknek a jegyzéke itt található).

Ennek a cégnek a termékeit vonta nagyító alá az ismert osztrák biztonságtechnikai cég, a **SEC Consultant**, és találtak is néhány igazán nyugtalanító dolgot; illetve hát szinte csak nyugtalanító dolgokat találtak.

A szakértők már az 2016-os **Mirai botnet** botnet támadása kapcsán felismerték, hogy az internetre számolatlanul csatlakozó IoT eszközök IoT – kamerák, multimédia-eszközök,.. – nagyon komoly veszélyt jelentenek; a SEC főleg ebből a szempontból vizsgálta meg Xiongmai eszközeit.

A cég kamerái egy saját felhőbe felhő csatlakoznak (XMEye P2P Cloud) automatikusan, például innen

kapják az automatikus szoftver-frissítéseket. A kutatók a kamerák firmware-nek firmware a visszafejlésével és az MAC címek ismeretének MAC olyan eljárást fejlesztetek ki, mely megvizsgálta a felhőbe csatlakozó kamerák sérülékenységét.

Csili-vili Xiongmai villanyégőbe integrált, mobil-telefonról elérhető kamera. Biztonság? Ehh, kit érdekel...

Összesen **16 millió kamerát** azonosítottak, ezek közül 9 millió volt folyamatosan a neten, megbecsülték, hogy csak Németországban 1,3 millió ilyen készülék van.

A készülékeken a rendszergazda-jelszó üres, és nem is szükséges ezt megadni; a legtöbb felhasználó valószínűleg nem is foglalkozik ezzel. Pedig ennek a jelszónak a birtokában valaki (vö. **bárki**) a kamera-képen kívül megtekintheti vagy aktiválhatja a videó-felvételeteket, megváltoztathatja az eszköz konfigurációját vagy letölthet firmware-t firmware is.

Ráadásul, ha még valaki annyira előrelátó, hogy megváltoztassa a jelszót, csak hamis biztonságérzete lehet, ugyanis van a kameráknak egy nem publikált felhasználója is (default) és a jelszava „tluafed” (default visszafelé), mellyel ugyanezeket a jogokat kapja meg a kamera felett.

A firmware megváltoztatása, azaz rosszindulatú behatolóval való kiegészítése bármikor lehetséges, ugyanis a frissítések nem tartalmaznak ellenőrző kódot (aláírást).

Az már csak tényleg hab a tortán, hogy a gyártó a készülékeihez „elfelejtett” saját MAC-cím tartományt MAC vásárolni, így néhány német cég (Protechna Herbst GmbH, Koenig & Bauer AG, Metrohm AG) címtartományait adta el sajátként.

Ez valami olyasmi a köznapi életben, mint amikor lusta vagyok az új kocsimra rendszámot venni, ezért leszerelem valakiét – mondván, neki úgy sem kell – és azt használom.

Elvileg az un. MAC-címeknek egyedinek kell(ene) lenniük az interneten, mint a fenti hasonlatban a rendszámoknak; de nyilván sok kínai gyártó igencsak hasonló hozzáállása sokat ront az összképen. A SAC mindenesetre felvette a gyártóval a kapcsolatot, akik ígéretet tettek arra, hogy legalább a trükkös „default” felhasználót törlik a firmware-ből.

Fordítsuk le a történetet *„emberi”* nyelvre; miért is veszélyes a fenti Xiongmai kamerák használata?

1. Mert bárki benézhet a házunkba a jelszavak ismeretében vagy a már módosított firmware-en keresztül. Videofelvételeket készíthet és érzékeny felvételek esetén megzsarolhat minket (például a napiszarral).
2. A behatoló – ha még előttünk megváltoztatja a kamera jelszavát – gyakorlatilag kizár minket a saját kameránkból.
3. A firmware módosításával kameránk egy zombi (vagy ha úgy tetszik bot) lesz egy botnet botnet hálózatban.
4. A hálózaton duplán, vagy sokszorosan jelenlevő MAC-címek azonosítási problémákat eredményezhetnek (jó, ennek meglehetősen csekély a valószínűsége)

A fő probléma viszont ezzel a történettel az, hogy ez csak egy kínai gyártó egy terméke. Teljesen meg tudunk zuhanni az új, tömegével a piacra kerülő kütyüktől, anélkül hogy igazán bármit is tudnánk róluk. Ez csak egy történet volt, aminek szerintem az a tanulsága, hogy igenis megéri egészséges paranoiával közelíteni ezt a szép új világot.

Ajánló

Hasonló jellegű bejegyzéseket a **cyberwar** tag alatt talál:

- A Davis-Besse atomerőmű esete a vírussal 2026/06/26 20:42
- A Stuxnet sztori 2026/06/26 20:43
- A Supermicro történet 2026/06/26 20:43
- A Trans-Szibéria gázvezeték 1983-as robbanása 2026/06/26 20:43
- A Világ valódi csodái 2026/06/26 20:45
- Krétával és palatáblával a zsarolóvírus ellen 2026/06/26 20:45
- Xiongmai sztori 2026/06/26 20:46

Kedves olvasóm! Ha már idáig eljutottál az olvasásban, talán joggal feltételezhetem, hogy nem volt

teljesen érdektelen számodra ez a bejegyzés. Jaj, le ne ixelj még; nem pénzt akarok tarhálni.

Pusztán annyit kérek, hogy ha van olyan ismerősöd, akivel jót tudnál vitatkozni az itt leírtakról, vagy csak simán megosztanád vele, kérlek, ne késlekedj!

Továbbra is keresek megjelenési lehetőséget az írásaim számára. Ha esetleg van ötleted, osszd meg velem! Elérhetőségeim az Impresszumban találhatók.

A passport.blog jelenlegi egyetlen megjelenési lehetősége a Facebook. Ha értesülni szeretnél az új bejegyezésekről, kövesd a Bolyongó Facebook oldalt.

Ha szeretnéd a bejegyzést kinyomtatni, vagy önálló formában menteni, ennek a legegyszerűbb módja a PDF formába konvertálás. Ezt a jobb oldali, fentről negyedik (Adobe) ikonnal teheted meg.

Eddigi bejegyzések a bolyongó.hu-n

Az összes bejegyzés ABC-be rendezett indexe itt található. A blog helyekhez köthető bejegyzései a google.maps térképen is megtalálhatók: A világ valódi csodái. A mostanában a blogon megjelent írások a főoldalon jelennek meg.

2026/05/28 16:05

Forrás

A fenti bejegyzést a golem.de Millionen IoT-Kameras immer noch angreifbar im Netz bejegyzése alapján írtam.

mobiltelefon, kamera, malware, zombi, botnet, cyberwar, iot, 2018, Kína, Xiongmai, SEC Consultant, biztonság, tech, felhő, cloud, MAC, great bugs

Bejegyzésmegtekintések száma: 5