HACKLI SME VÝŤAH



ISECO



ĽUBOMÍR KOPÁČEK

CERTIFIKOVANÝ AUDÍTOR KB

ETHICAL HACKER

CYBER SECURITY ADVISOR



HACKLI SME VÝŤAH?

- Dobrá správa je že nie
- Moderné výťahy ale majú dnes všetko, čo je k úspešnému útoku potrebné
- Pozrieme sa aj na PoC ako ~~by~~ to je možné



VÝBUŠNÝ KOKTEJL

- Riadiaci systém
- Gateway, modemy, vzdialený prístup
- Cloud, monitoring, diagnostika
- Servisný notebook (celé zle...)
- Servisné firmy (ešte horšie)
- Prepojenie na BMS/BAS, EPS, video, hlas, obosjmerná komunikácia

PARADOX

ČÍM JE VÝŤAH INTELIGENTNEJŠÍ

A VIAC MONITOROVANÝ, TÝM JE

ZRANITEĽNEJŠÍ



4 VSTUPNÉ BODY

- Vzdialený servis (čo vieme o jeho bezpečnosti? čo vôbec o ňom vieme?)
- Servisný notebook (evergreen... A.K.A. notebook pre celú rodinu)
- Zdieľaná sieť s inými technológiami (kde sú bezpečnostné zóny?)
- Zraniteľné komponenty (PLC, aktívne prvky, čokoľvek...)

INCIDENT

NIE JE OTÁZKA ČI, ALE KEDY...



EXPERTI ZISTILI...

- Samotná technológia výťahu nemusí byť cieľom útoku, ale slúži ako “Pivot Point” – skok do iných systémov
- Nie nie je to “v pohode”, útočník nerieši kolaterálne škody, ktoré môžu byť pre prevádzku fatálne

KONVERGENCIA

EXPRESNÁ CESTA DO PEKLA,

OBČAS DOSLOVA...



NORDIC CHOISE HOTELS

- Ransomverový útok na sieť hotelov Nordic Choise Hotels
- Sekundárny dopad aj na prevádzku výťahov “našťastie” iba na úrovni autentifikácie hotelovými kartami (oficiálne...)



ĎALŠIE PRÍPADY

- MGM Resorts Las Vegas – útok na hotel, výťahy sa “zbláznili” kvôli nefunkčnému access control, prevádzku riadila ochranka hotela ;)
- Útoky na konvergované siete, špeciálne v hoteloch sú pomerne časté
- Útoky na BMS/BAS alebo access control často “berú so sebou” aj výťahy, zatiaľ bez zdokumentovaného dopadu na safety logiku (veríme tomu?)

POC

VOJNA JE SKVELÉ

LABORATÓRIUM



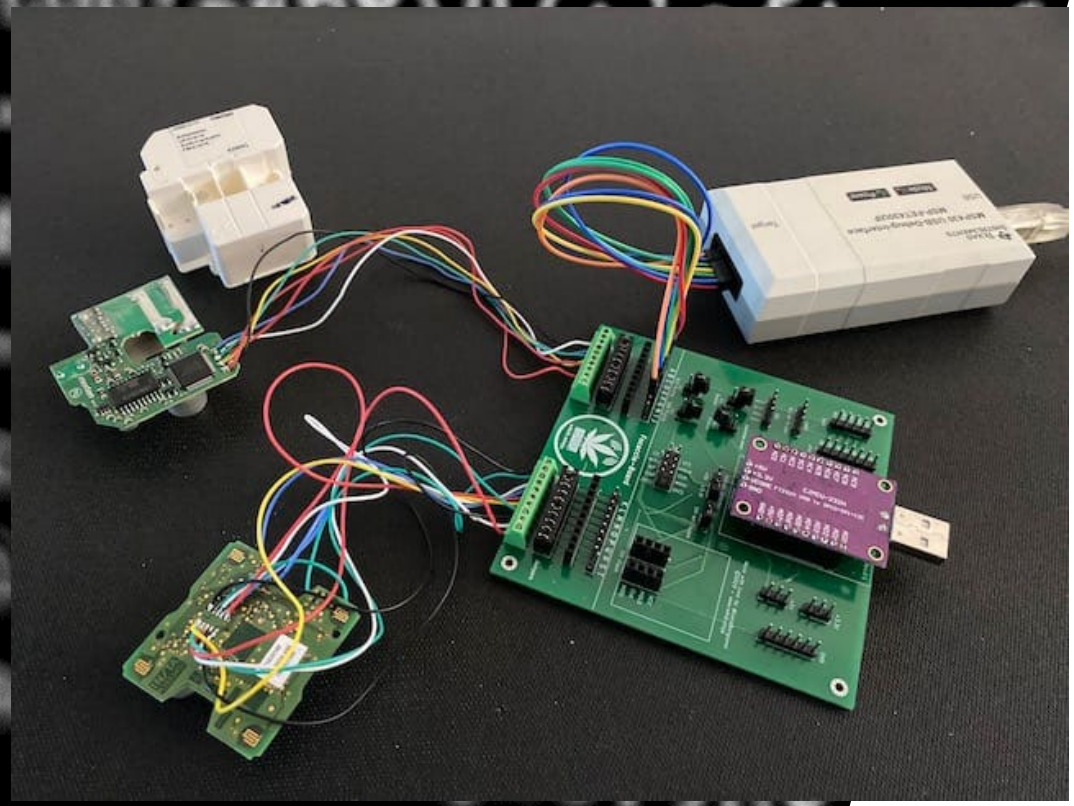
TEKON AVTOMATIKA

- Prvý zdokumentovaný cielený útok priamo proti výťahovým PLC systémom
- Výťahy ako také boli len bočný efekt, v skutočnosti boli PLC zneužité ako Pivot Points
- Pro-ukrajinská skupina Lifting Zmiy realizovala úspešné útoky proti OT cielom v Rusku, špeciálne so zameraním na PLC ruského výrobcu Tekon Avtomatika
- Údajne bez fyzického poškodenia vyťahov, avšak zdroje informácií nie sú dôveryhodné

KEĎ

SI STRELÍME DO

VLASTNÉHO KOLENA



ÚPLNA STRATA KONTROLY

- Jeden z najväčších BAS (Building Automation Systems) incidentov na svete, Nemecko 2021
- Správcovia BAS stratili kontrolu nad stovkami systémov (vrátane výťahov) po krádeži digitálnych bezpečnostných kľúčov. BAS zariadenia zostali kompletne “bricknuté”
- Hovorí sa o úspešnom “handover” (prebratí kontroly) nad BAS systémami útočnikmi
- Správca doplatil na “asi” nesprávne implementovaný key management = riešenie bolo až tak bezpečné, že sa doň nedokázal dostať ani výrobca...
- Výrobca musel nakoniec hacknúť svoje vlastné zariadenia a pokúsiť sa o extrakciu kľúčov

ČO S TÝM?



"ORIGINÁLNE" RADY

- Plánujte
- Testujte
- Penetračne testujte
- Vzdelávajte vývojarov
- Vzdelávajte servisných technikov
- Lebo odborník na IT ≠ odborník na bezpečnosť

ĎAKUJEM

WWW.ISECO.SK

ISECO