

HROZBA V ROZKROKU!

Ášter½, 04 kvÁten 2021

IOT (Internet of Things) zaÁ™-zenÁ-, tedy ta, která; lze nÁ› jak½m zpÁ-sobem pÁ™ipojit do internetu, postupujÁ- do vÁ›ech od vÁ›tvÁ-. Dokonce i mezi erotickÁ© pomÁ-cky. A jeliko¾ je situace kolem zabezpeÁ-enÁ- nÁ› kterÁ½ch IOT zaÁ™-zenÁ- á- mÁ-Á¾e tak bÁ½t âœœveseloâœœ i v rozkroku. V bÁ™eznu se napÁ™-klad objevila velká; anal½za spoleÁ-nosti ESET, která; na chyby v tÁ›chto dvou hraÁ-kÁ›ch pro dospÁ›lÁ©:

Slo¾itÁ›jÁ›- ne¾ bezdrÁ›tovÁ© otevÁ-rÁ›nÁ- vrat

RizikovÁ½ch mÁ-st je tam dokonce vÁ-ce ne¾ u typickÁ©ho IOT zaÁ™-zenÁ- pro bezdrÁ›tovÁ© otevÁ-rÁ›nÁ- garÁ›¾ovÁ› zapÁ-nÁ›nÁ- svÁ›tel. NavÁ-c se toti¾ v yuÁ¾vÁ›; lokÁ›lnÁ- bluetooth komunikace mezi mobilnÁ- aplikacÁ- a âœœhraÁ-kouâœœ ovlÁ›dnÁ›nÁ- nevstupuje jen uÁ›ivatel erotickÁ© hraÁ-ky, ale i potenciÁ›lnÁ- partner, která½ mÁ-Á¾e sedÁ›t Á›plnÁ› jinde a mÁ-pindÁ-ka / pipinku pod vzdÁ›lenou kontrolou. Á¾e mÁ-Á¾e bÁ½t nÁ› jakÁ› chyba i v samotnÁ© komunikaci mezi cloudem a mobilnÁ- aplikacÁ- nebo v samotnÁ© cloudovÁ© slu¾bÁ›, to je vÁ›eobecnÁ© riziko jakÁ©hokoliv IOT zaÁ™-zenÁ-.

Do rozkroku vstup povolen

PrvnÁ- objevenÁ½ problÁ©m je uÁ¾ v bluetooth komunikaci mezi hraÁ-kou a telefonem, kdy se lze do pÁ›rovÁ›nÁ- vnutit jak½mkoliv cizÁ-m zaÁ™-zenÁ-m v dosahu a neexistuje tam Á¾Á›dnÁ½ autorizaÁ-nÁ- proces. Tady tak lze uplatnit Á›tok typu MitM (Man in the Middle), kdy mezi hraÁ-kou a mobilnÁ-m telefonem uÁ›ivatele figuruje zaÁ™-zenÁ- Á›toÁ-nÁ-ka, která© komunikaci odchytÁ›vÁ›i nebo do nÁ- vhodnÁ› vstupuje.

U zaÁ™-zenÁ- Lovense navÁ-c bylo mo¾nÁ© uplatnit brute-force Á›tok z internetu a zkusit tak vzdÁ›lenÁ› ovlÁ›dnout pÁ›vÁ› zapnutÁ© cizÁ- hraÁ-ky tohoto vÁ›robce. To bylo mo¾nÁ© dÁ-ky nedostatÁ-nÁ© unikÁ›tnosti tokenÁ- jednotlivÁ½ch zaÁ™-zenÁ- která© mohou bÁ½t ovladatelnÁ© pÁ™es URL <https://api2.lovense.com/c/<TOKEN>>. To, Á¾e existuje i skupina uÁ›ivatelÁ-, k vlastní- token sdÁ-lÁ- veÁ™ejnÁ›, to snad ani nebudu rozebÁ-rat.

NaÁ›lo se jeÁ›tÁ› pÁ›r dalÁ›ch nedostatkÁ-, nicmÁ©nÁ› vÁ›e je popsÁ›no v Á›lÁ›nku âœœSex in the digital era: How secure are sex toysâœœ na Welivesecurity.com a pÁ™ilo¾enÁ© PDF zprÁ›vÁ›, vÁ›etnÁ› nÁ›kolika video ukÁ›jek.

IOT

pÁ›s cudnosti: Zamknout pÁ™es internet, odemknout bruskou!

Tohle vÁ›echno je ale nic proti IOT pÁ›su cudnosti âœœCellmate Chastity Cageâœœ od spoleÁ-nosti Qiui, která½ byl v minulÁ©m testovÁ›n organizacÁ- Pen Test Partners. Tam toti¾ bylo technicky mo¾nÁ© pÁ™evzÁ-t kontrolu nad vÁ›emi aktivnÁ-mi pÁ›s cudnosti v horizontu nÁ›kolika dnÁ-. Bylo tak mo¾nÁ© zÁ-skat citlivÁ© informace uÁ›ivatelÁ- pÁ›sÁ- (jejich skuteÁ-nÁ© jmÁ© telefonnÁ- Á-Á-slo, datum narozenÁ-, lokalitu z GPS, âœœ), ale tÁ©¾ pÁ›s cudnosti pÁ™es internet zamknout!

A teÁ- pozor! ZaÁ™-zenÁ- bylo mo¾nÁ© pÁ™ivÁ©st do stavu, kdy bylo pÁ™es internet zamknuto a nebylo ho mo¾nÁ© o ne¾ fyzickÁ½m zÁ›sahem.

A zde pozor podruhÁ©: tento pÁ›s cudnosti nemá; Á¾Á›dnou fyzickou pojistku ani mechanismus pro nouzovÁ© otevÁ™enÁ-! ZÁ›mek je navÁ-c natolik poctivÁ½, Á¾e existujÁ- vlastnÁ› jen dvÁ› Á™eÁ›jenÁ-, jak tuhle vÁ›c z âœœpiÁ-Á-ouruâœœ sundat:

- PouÁ¾Á-t Á›hlovou brusku ala flexu a doufat, Á¾e si kromÁ› pÁ›su cudnosti neuÁ™-znete i nÁ›co jinÁ©ho.
- MÁ-t nÁ›koho Á›jikovnÁ©ho k ruce (spÁ-Á›je k noze), kdo noÁ¾em vyÁ™-zne (pÁ™ipevnÁ›no lepidlem) a vydloubne sprÁ›vnÁ› plastu, a na sprÁ›vnÁ© vodiÁ-e uvnitÁ™ poÁ›le pÁ™esnÁ› 3 volty, která© zpÁ-sobÁ- otevÁ™enÁ- zÁ›mku.

Ransomware: chceÁ› to odemknout? ZaplaÁ›! TÁ™eÁ›niÁ-kou na dortu je, Á¾e na github.com byl dokonce nalezen zdrojovÁ½ kód ransomwaru (napsanÁ½ v Pythonu), která½ pÁ›vÁ› tuto fatÁ›lnÁ- chybu v komunikaci zneuÁ¾vÁ›i a dokÁ¾e hromad pÁ›sy cudnosti zamknout. A jak to uÁ¾ u ransomwaru bÁ½vÁ›i, do mobilnÁ- obslu¾nÁ© aplikace doruÁ-Á- vzkaz, Á¾e pokud

odemknout, je potřeba nejprve zaplatit (například v bitcoinech)!

IGOR HÁK

<https://viry.cz/>