ŠKODLIVÝ SOFTVÉR V ZARIADENÍ

MALVÉR AKO HROZBA MODERNÉHO DIGITÁLNEHO ŽIVOTA

V dnešnej digitálnej dobe je ochrana našich zariadení mimoriadne dôležitá. Mobilné telefóny, tablety a počítače už dávno neslúžia len na komunikáciu – uchovávajú citlivé informácie o nás samých, o našej rodine aj o našej práci. Nachádzajú sa v nich osobné fotografie, kontakty, pracovné dokumenty, prístupové údaje k sociálnym sieťam, e-mailom či internetovému bankovníctvu. Úspešným útokom získa útočník prístup k nášmu celému virtuálnemu životu. Jeho ziskom sa stávajú naše osobné údaje, súkromie, dáta a v konečnom dôsledku aj financie, ktoré prostredníctvom daného zariadenia spravujeme. Malvér tak nepredstavuje len technický problém, ale zásah do osobnej bezpečnosti a stability jednotlivca.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Mechanizmus útoku pomocou škodlivého softvéru

Podvodníci najčastejšie šíria škodlivý softvér prostredníctvom podvodných aplikácií. Tie sa vydávajú za bežné alebo užitočné nástroje, ako sú optimalizátory systému, bezpečnostné aplikácie, prehrávače, prípadne napodobňujú aplikácie známych spoločností vrátane bánk. Po stiahnutí do zariadenia aplikácia žiada používateľa o udelenie veľkého množstva oprávnení, ktoré nie sú potrebné pre jej deklarovanú funkciu. Ide napríklad o prístup k SMS správam, súborom, mikrofónu, kamere alebo dokonca k zobrazeniu obrazovky.

Po udelení týchto oprávnení získa aplikácia prakticky úplnú kontrolu nad zariadením. Škodlivý softvér následne monitoruje činnosť používateľa, kopíruje prihlasovacie údaje, zachytáva SMS správy s overovacími kódmi a umožňuje podvodníkom vzdialene zadávať platby alebo manipulovať s bankovou aplikáciou. V niektorých prípadoch malvér pracuje nenápadne na pozadí bez viditeľných prejavov, takže používateľ si kompromitáciu zariadenia nemusí dlhý čas všimnúť. Práve táto skrytá činnosť robí malvér mimoriadne nebezpečným.

Indikátory prítomnosti malvéru v zariadení

Existuje viacero varovných signálov, ktoré môžu naznačovať, že zariadenie je infikované škodlivým softvérom. Prvým indikátorom je aplikácia ponúkaná mimo oficiálnych obchodov, ako sú Google Play alebo App Store. Podozrivé je aj to, ak inštalovaná aplikácia vyžaduje neprimerané množstvo oprávnení bez zjavného dôvodu.

Po inštalácii sa zariadenie môže správať nezvyčajne – reaguje pomalšie, prehrieva sa alebo zobrazuje neznáme upozornenia. Výstražným znakom je aj neštandardné správanie bankovej aplikácie, napríklad časté chybové hlásenia alebo výpadky. Zvlášť nebezpečné sú situácie, keď sa platby potvrdzujú automaticky a používateľ si všimne problém až po zmene zostatku na účte.

Ako sa chrániť pred malvérom

Základnou ochranou je inštalovať aplikácie výhradne z oficiálnych obchodov a overovať si ich hodnotenia, recenzie a vývojára. Používateľ by mal dôkladne kontrolovať oprávnenia aplikácií a odmietnuť tie, ktoré sú zjavne neprimerané. Dôležité je pravidelne aktualizovať operačný systém aj aplikácie, keďže aktualizácie často opravujú bezpečnostné chyby.

Odporúča sa používať kvalitný antivírusový softvér a neklikať na podozrivé odkazy v správach či e-mailoch. V prípade podozrenia na infekciu je vhodné okamžite odpojiť zariadenie od internetu, kontaktovať banku a zvážiť odbornú kontrolu alebo obnovenie zariadenia do továrenských nastavení.

Útok typu škodlivý softvér v zariadení je mimoriadne nebezpečný, pretože útočník získava prístup k celému digitálnemu životu obete. Malvér dokáže nenápadne sledovať činnosť a kradnúť citlivé údaje bez vedomia používateľa. Následky môžu zahŕňať stratu dát, súkromia aj financií. Ochrana pred týmto typom útoku si vyžaduje obozretnosť a zodpovedný prístup k používaniu zariadení. Prevencia je vždy jednoduchšia a menej bolestivá než riešenie následkov úspešného útoku.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti