Budapest, 2016. március 28. - **Internetkapcsolat nélküli adatlopási módszert fedeztek fel az ESET szakemberei, amelyhez elegendő csupán egy fertőzött USB adathordozó.**

Az ESET és a szintén IT-biztonsággal foglalkozó Sicontact Kft. közös közleménye szerint az USB Thief-re keresztelt trójai kártevő kizárólag USB kulcsokon terjed, anélkül hogy bármilyen bizonyítékot, vagy nyomot hagyna a fertőzött számítógépeken. Az alkotói speciális működési mechanizmust alkalmaznak, ami még nehezebbé teszi a kártevő másolását, felderítését és elemzését. Rejtett támadásaival képes az elkülönítetett hálózatokon lévő adatok eltulajdonítására, ráadásul a felderítés és visszafejtés ellen is védi magát.

A kártevő a hordozható alkalmazások - mint például a Firefox, Notepad++, Truecrypt - plugin forrásában (a szoftvert és hardvert bővítő vagy módosító kiegészítő modulforrás), vagy az alkalmazás által használt DLL-ben (Dynamic Link Library - dinamikus csatolású könyvtár) tárolódik, és a fertőzött alkalmazás indításával a kártevőt is élesíti a háttérben a felhasználó.

A Sicontact Kft. közölte: egy partnerei körében végzett felmérése szerint a mintegy 1800 válaszadó 21 százaléka talált már más által elhagyott adathordozót, és nagy többségük meg is nyitotta ezek tartalmát. A kft. vezető IT tanácsadója, Béres Péter szerint ezért a biztonsági megoldások használata mellett nagyon fontos az is, hogy a felhasználók megértsék, egy ismeretlen vagy nem ellenőrzött forrásból származó USB milyen veszélyeket rejthet. Amíg ez nem így lesz, addig a számítógépek, illetve az izolált hálózatok is folyamatos veszélynek vannak kitéve - idézte a közlemény a tanácsadót.