EGOSECURE
ENJOY DATA PROTECTION

BadUSB – Vlk v rouše beránčím

Ochrana proti malwaru BadUSB pomocí EGOSECURE

Výzva pro bezpečnost

Malware zvaný BadUSB už se světovými počítači pohybuje několik let; jde o běžný a účinný způsob útoku, který dokáže ohrozit jakoukoli organizaci. BadUSB je USB flash paměť plná malwaru, tedy škodlivého softwaru. Je maskovaný, a protože se chová jako klávesnice, nenaleznou ho žádné antivirové programy ani jiné ochranné mechanismy. V přestrojení za zdánlivě obyčejnou klávesnici dokáže v podstatě ovládnout počítač a provádět libovolné příkazy. Mezi několik příkladů jeho chování patří navázání spojení s jinými počítači, spouštění ransomwaru a mazání nebo šifrování souborů uložených na pevném disku. Může také zkopírovat data na flash paměť, kterou obsahuje, nebo dokonce do cloudu.

Z pohledu zločinců jde o skvělý nástroj. K vytvoření skriptu pro BadUSB nejsou potřeba žádné znalosti programování. Lze jej jednoduše vytvořit na snadno dostupných webových stránkách, díky čemuž je BadUSB pro „zlé hochy“ ještě přitažlivější.

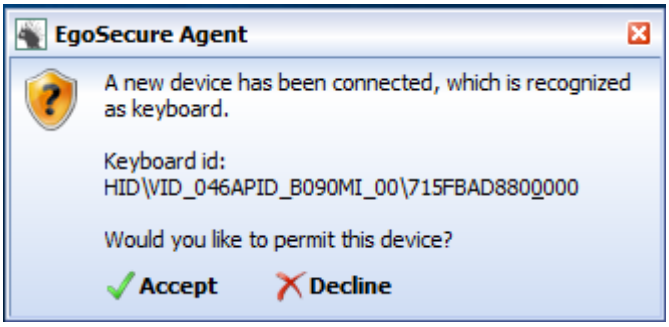
Jednoduché řešení nestačí

Někteří uživatelé se domnívají, že nakažení malwarem z tohoto zdroje lze zabránit účinnou správou zařízení – stačí určit, jaké USB flash paměti lze ve firmě používat, a všechny ostatní, včetně BadUSB, zablokovat.
Jenže tak snadné to není. Problém je, že BadUSB je ve skutečnosti rozpoznán jako klávesnice.
A klávesnici běžně používá každý počítač. Jednoduchá správa zařízení tedy sama o sobě nefunguje.
Jediným řešením je podrobně se podívat na způsob útoku a vytvořit speciální ochranu.

EGOSECURE
ENJOY DATA PROTECTION

Ochrana proti malwaru BadUSB pomocí EGOSECURE

Krátce po prvních zprávách o BadUSB byla do systému EgoSecure Data Protection doplněna speciální funkce nazvaná „Ochrana proti BadUSB“. Základem této ochrany je zabránit v používání nepovolené druhé klávesnice.



Nestačí k tomu však jednoduché zablokování. To by nefungovalo, protože mobilní počítače mají klávesnici vestavěnou a běžně používají dokovací stanice nebo externí klávesnice. Autorizaci klávesnic lze tedy řešit jedině pomocí seznamů povolených zařízení.

Víme, že správa takových seznamů může být pro administrátory prací navíc. Vzhledem ke škodám, které mohou následkem útoků malwaru BadUSB vzniknout, je ale nějaké úsilí evidentně potřeba. Ve společnosti EGOSECURE jsme hrdí na to, že se naše produkty snažíme udržovat co nejjednodušší. Naše řešení tedy od administrátorů vyžaduje jen minimum další práce.

Správa je snadná a zároveň flexibilní – pro administrátora i pro uživatele. Jednou z možností je, že administrátor okamžitě a jednoduše povolí použití všech klávesnic, které jsou v danou chvíli připojeny. Alternativně může povolit seznam používaných klávesnic převzatý z modulu inventáře. Položky na seznamu lze podle potřeby přidávat a odebírat. Aby to bylo ještě snazší, lze tento postup doplnit o povolování bez zásahu administrátora – uživatel ostatně nejlépe ví, zda bude používat druhou klávesnici, nebo ne. Až do dokončení povolovacího procesu je druhá klávesnice zablokována.

Nezáleží na tom, zda si vyberete povolování uživatelem nebo správu administrátorem, případně obojí. Se systémem EGOSECURE je možné cokoli. Stačí několik kliknutí myší a jednoduše a flexibilně vytvoříte účinnou ochranu proti útokům malware BadUSB.

EGOSECURE – Jednoduché a snadné řešení

Díky svému systému EgoSecure Data Protection je německá bezpečnostní firma EGOSECURE již více než 10 let předním hráčem na poli inovací v oblasti komplexních řešení ochrany dat. Zabezpečujeme data na všech koncových bodech v celém firemním procesu. A jak jistě očekáváte, splňujeme aktuální zákony a oborové normy.

EGOSECURE je světově prvním výrobcem, který spojil analýzu dat a ochranné moduly do jednoho řešení. Obě části jsou hladce integrovány do jediného řešení prostřednictvím managementové konzole, společné databáze, jediné instalace a metodologie správy. Díky tomu je instalace rychlá, správa snadná a stačí jen minimální školení uživatelů. To vše v souladu s naším sloganem „Zjednodušujeme složité věci“.

FREEDIVISION
for safety reasons

Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

Telefon: +420 220 972 426
E-mail: info@freedivision.com
www.freedivision.com