Pozor na SMS zprávy. V Česku se přes ně šíří bankovní virus

Na pozoru by se měli mít lidé před SMS zprávami, které v posledních dnech obdrželi od neznámých zdrojů. Bezpečnostní experti antivirové společnosti Eset v úterý varovali před novou vlnou virů, které se šíří právě prostřednictvím SMS zpráv. Útočníci se snaží dostat se k penězům na cizích bankovních účtech.

Kyberzločinci využívají stejnou taktiku, kterou již koncem ledna zkoušeli v Německu pod hlavičkou bank. Tehdy se soustředili výhradně na tamní uživatele. Aktuálně byla hrozba lokalizována i v češtině a šíří se v tuzemsku.

„Na Česko cílí nová vlna malwaru, který se šíří podvodnými zprávami SMS. Podle aktuálních informací se útočníci prozatím zaměřili jen na ČSOB. Dá se však očekávat, že okruh cílových bank se brzy rozšíří," podotkl Lukáš Štefanko, analytik malwaru ve společnosti Eset.

Problém představuje nabízená aplikace

Jak vlastně útok probíhá? Součástí došlé zprávy je odkaz na stažení mobilní aplikace. Ta na první pohled nemusí s internetovým bankovnictvím vůbec souviset.

„Tento nebezpečný malware se maskuje za údajnou aplikaci společnosti DHL, která však stáhne podvodnou aplikaci s názvem ‚Flash Player 10 Update' a ikonou společnosti DHL," konstatoval Štefanko.

Problém představuje právě aplikace, kterou podvodníci prostřednictvím SMS zprávy propagují. Jde totiž o trojského koně, který při otevření internetového bankovnictví podsune falešnou přihlašovací stránku. Uživatelé tak naservírují počítačovým pirátům přístup k účtu jako na zlatém podnosu.

A vzhledem k tomu, že pachatelé již mají přístup i k mobilnímu telefonu, kam zpravidla chodí potvrzovací SMS zprávy k proběhlým transakcím, už jim nic nebrání ve vybílení účtu.

Zkoušeli to už dříve

Stejnou taktiku zkoušeli kyberzločinci na konci ledna i v Česku – tehdy se však vydávali za zaměstnance internetového obchodu Alza.cz a slibovali důvěřivcům poukaz v hodnotě 500 Kč. I tehdy šlo ale pochopitelně o podvod. [celá zpráva]

„K omezení rizik doporučuji dodržovat především dvě základní bezpečnostní opatření. V prvé řadě je nutné nenechat se přimět k instalování aplikací pomocí odkazů, které mohou vést na podvodnou stránku. Aplikaci, kterou chce uživatel instalovat, je třeba si vždy vyhledat v oficiálním obchodě s aplikacemi nebo na důvěryhodných stránkách," vysvětlil Lukáš Štefanko.

Aktuální hrozba se týká výhradně přístrojů s operačním systémem Android. Není nicméně vyloučeno, že stejným způsobem se budou kyberzločinci snažit dostat i do přístrojů postavených na jiných platformách.

Na chytré telefony se zaměřují počítačoví piráti v posledních měsících stále častěji. Uživatelé na těchto přístrojích totiž velmi často podceňují bezpečnost.

Aby majitel omezil rizika, měl by svůj smartphone vybavit podobně jako stolní počítač antivirovým programem a měl by pravidelně stahovat všechny důležité aktualizace nainstalovaných aplikací i samotného operačního systému.