Přehled hrozeb pro Android: V květnu byly zdrojem adwaru a bankovního trojského koně hry pro nejmenší uživatele

19.6.2024 - Lucie Mudráková | ESET software

Adware Andreed a bankovní trojský kůň Cerberus byly i v květnu hlavními kybernetickými hrozbami pro platformu Android v Česku. Doplnil je opět škodlivý kód se špionážními funkcemi.

Jednalo se tentokrát o downloader Agent.CZB. Všechny nejčastěji detekované škodlivé kódy se v květnu šířily prostřednictvím falešných verzí aplikací pro chytré telefony. V případě adwaru a bankovního trojského koně to byly především mobilní hry, a to často zacílené na nejmenší uživatele z řad dětí. Bezpečnostní specialisté tak upozorňují, že s příchodem léta může být i tato skupina zvlášť zranitelná. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET.

Adware Andreed zůstal i v květnu v čele pravidelné statistiky hrozeb pro platformu Android v Česku. Bezpečnostní specialisté pozorují v jeho případě zatím stejný vzorec, jako vloni před začátkem prázdninové sezóny - Andreed se šíří prostřednictvím falešných verzí různých her, a to většinou i pro ty nejmenší uživatele z řad dětí. V květnu se pak navíc objevil také v aplikacích nabízejících luštění křížovek.

„Letní období bývá pro uživatele obecně více nebezpečné, a to proto, že vlivem letních dovolených, výletů a více prostoru pro volnočasové aktivity mohou polevit ve své ostražitosti vůči nástrahám digitálního světa," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. „Opakovaně v tomto období také pozorujeme, že kyberbezpečnostní rizika se nevyhýbají ani dětem. Ty budou mít s příchodem prázdnin také větší prostor k tomu, aby povinnosti vyměnily právě například za hraní her. Adware je pak pro zacílení na děti ideální. Po stažení do zařízení se může chovat velmi nenápadně a projevit se až po čase. Vyskakující agresivní reklamy ale mezitím mohou nabízet uživatelům nebezpečné odkazy. Pokud na ně kliknou, mohou se dostat na nebezpečné a podvodné webové stránky. S příchodem letních prázdnin je tak určitě vhodné děti poučit o těchto rizicích," dodává Jirkal.

Také v květnu se v čele statistiky nadále držel bankovní trojský kůň Cerberus. Ve vyšším počtu detekcí se v Česku začal objevovat před několika měsíci. Stále se šíří především prostřednictvím neoficiální verze hry Fast Car Driving - Street City.

„Kombinaci adwaru s bankovním trojským koněm jako dvou největších hrozeb vidíme již několikátým měsícem. Trojský kůň Cerberus se také šíří prostřednictvím mobilních her, už se však jedná o závažnější typ malwaru, který je rizikem zejména pro internetové bankovnictví. Dlouhodobá přítomnost adwaru a zatím opakované detekce trojského koně svědčí o tom, že se zcela evidentně jedná o úspěšné škodlivé kódy, jejichž využívání se útočníkům stále vyplácí," říká Jirkal.

Zatímco počet detekcí malwaru Spy.SpinOk s prvky spywaru v květnu znatelně klesl, vystřídal ho na třetím místě statistiky downloader Agent.CZB. Nejvíce případů tohoto škodlivého kódu zachytili bezpečnostní experti 24. května. Uživatelé a uživatelky na něj mohli narazit ve verzi aplikace na malování ibisPaint.

„Návrat aplikací se špionážními prvky můžeme sledovat již od dubna, kdy se opět objevil malware Spy.SpinOk. Downloader Agent.CZB stahuje z internetu další škodlivý kód, který pak nepozorovaně dokáže spustit v našem zařízení. Útočníci mohou jeho prostřednictvím pravděpodobně také zobrazovat adware, převzít kontrolu nad telefonem nebo získávat ze zařízení informace," vysvětluje Jirkal.

V obraně před kybernetickými hrozbami je klíčová naše ostražitost v kombinaci s komplexním bezpečnostním řešením. Bezpečnostní experti doporučují, aby uživatelé kybernetická rizika nepodceňovali ani v letním období.

„Většinou to není tak, že by kyberútočníci v letním období vynakládali více času a energie na vývoj nových hrozeb a nových strategií, přesto je toto období pro uživatele více nebezpečné. Nastává zkrátka více příležitostí pro to, aby se škodlivý kód dostal do jejich zařízení. Kromě neuváženého stahování aplikací z neprověřených obchodů třetích stran a internetových fór se s létem pojí ještě další rizika. Jsou to například veřejné Wi-Fi sítě na letištích, v hotelech a kavárnách, které nejsou dostatečně zabezpečené před zneužitím. Takovému útoku se říká man-in-the-middle, což v češtině znamená člověk uprostřed. Hackeři jeho prostřednictvím dokáží překonat šifrování sítě a odposlouchávat tak naši komunikaci," říká Jirkal a dodává: „V neposlední řadě je toto období ideální pro to, abychom zavedli řeč na téma kybernetické bezpečnosti také s našimi dětmi. Doporučoval bych jim v základu vysvětlit, s jakými riziky se mohou na internetu setkat a na co si dávat v online prostředí pozor."

Nejčastějším rizikům pro děti na internetu se věnuje také iniciativa Safer Kids Online, která má za cíl pomoci jejich rodičům zorientovat se v nástrahách digitálního světa. Uživatele všech věkových kategorií bude před aktuálními hrozbami varovat také kvalitní bezpečnostní software. Ten dnes obsahuje řadu doplňkových funkcí, jako je například virtuální privátní síť (VPN) pro zabezpečené a soukromé prohlížení internetu.

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

Lucie Mudráková

Specialistka PR a komunikace
ESET software spol. s r.o.

tel: +420 702 206 705
lucie.mudrakova@eset.cz

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/prehled-hrozeb-pro-android-v-kvetnu-byly-zdrojem-adwaru-a-bankovniho-trojskeho-kone-hry-pro-nejmensi-uzivatele