ANTIVIROVÁ OCHRANA pro smartphony a tablety

V současné době existuje pro platformu Android asi milion škůdců, proti kterým jsou bezpečnostní mechanismy tohoto operačního systému bezmocné. Chip otestoval antiviry, které obranu zvládnou mnohem lépe.

JÖRG GEIGER

Bezpečnostní expert Chipu, který se specializuje na bezpečnostní hrozby pro mobilní zařízení.

Na začátku července 2013 byl objeven zásadní bezpečnostní problém pro operační systém Android. Bezpečnostní experti z BlueBox Security totiž odhalili nejzávažnější doposud známou mezeru v tomto oblíbeném mobilním operačním systému Googlu. Chyba umožňuje manipulovat s obsahem aplikace, bez vzniku jakýchkoli změn v jejím kontrolním součtu.

To v praxi znamená, že uživatelé systému Android už nemohou jednoduše zjistit, zda je daná aplikace původní, nebo zda se jedná o verzi obsahující například trojského koně. Takováto masivní slabina je přesně to, co autoři virů pro Android hledají, protože jim to umožňuje nepozorovaně šířit své viry a trojské koně mezi nic netušící uživatele. Tento problém ovlivní 99 procent všech zařízení se systémem Android, což znamená, že se týká přibližně 90 milionů smartphonů a tabletů po celém světě. Další špatnou zprávou pro uživatele OS Android je to, že rychlým tempem roste také počet malwarových hrozeb. Bezpečnostní odborníci z organizace AV-Test, která kontrolovala schopnost detekce v rámci tohoto testu, jich mají už plnou databázi.

Nedávno byla překročena hranice jednoho milionu virů a každý měsíc se objeví až 200 000 nových vzorků. Dobrou ochranu proti těmto virům tak mohou nabídnout pouze spolehlivé bezpečnostní aplikace, z nichž patnáct jsme v Chipu otestovali.

Od zdarma po 35 eur ročně

Testovací pole představovalo sbírku aplikací za cenu od 0 do 35 eur ročně, jejichž detekční antivirové schopnosti jsou skutečně impozantní. Všechny aplikace potřebují minimálně Android 2.1 nebo 2.2 a jsou kompatibilní se všemi následujícími verzemi až po nejnovější verzi OS. Laboratoř AV-Test použila pro testování detekčních schopností antivirů Android 4.2.2.

Potěšující zprávou je, že falešné antiviry, které se v obchodech s aplikacemi skrývaly pod názvy jako „Antivirus“ nebo „Guardian“ (ochránce) a které zcela postrádaly schopnost detekovat viry, jsou na ústupu. V každém případě ale platí, že pokud chcete investovat několik desítek eur do bezpečnostní aplikace, je vhodné držet se známých jmen. Naší kritice však neunikli ani někteří zavedení výrobci bezpečnostních nástrojů, a to díky strategii používání obchodu s aplikacemi. Většinu placených aplikací je možné si zdarma vyzkoušet – zkušební doba nejčastěji činí dva týdny nebo měsíc. To je na jednu stranu výborné, na druhou stranu bohužel většina výrobců zapomene na stránce v App storu zmínit, jak dlouhé je zkušební období a kolik bude ve finále stát roční poplatek. Na první pohled se tedy uživatelům může zdát, že aplikace je k dispozici zcela zdarma, během několika týdnů však přestane bezpečnostní balík pracovat a začne od uživatele požadovat peníze.

To nepovažujeme za příliš korektní jednání, a i proto v naší testovací tabulce nechybí položka s informací o nákladech na roční provoz.

Pouze jediná aplikace dokáže rozpoznat 100 procent malwaru

Existuje celá řada důvodů, proč si na mobilní zařízení pořídit bezpečnostní software, tím nejdůležitějším je ale pravděpodobně rostoucí počet malwarových hrozeb. Proto by i jedním z klíčových parametrů výběru antiviru měla být schopnost rozpoznat jednotlivé hrozby. I z toho důvodu nás překvapilo, že všechny malwary z testovací databáze (2 545 aplikací) dokázal rozpoznat jen jediný produkt – BitDefender Mobile Security. Pravda ale je, některé bezpečnostní nástroje se k této metě alespoň přiblížily: vítěz testu Trend Micro Mobile Security dosáhl úrovně detekce 99 procent, a MicroWorld eScan Mobile Security dokonce 99,9 procenta.

Z hlediska bezplatných aplikací si nejlépe vedl produkt od firmy Avast, který dosáhl úrovně detekce 99,8 procenta a jehož schopnosti jsou přibližně srovnatelné s placenými nástroji Symantec a Comodo. Naopak zcela zklamal bezplatný AegisLab Antivirus Free, jehož výkon byl daleko za ostatními – dokázal rozpoznat jen čtyři z deseti virů. Podle našeho názoru přináší takováto antivirová ochrana více problémů, než jich sama řeší.

V rámci ochrany v operačním systému Android jsou viry obvykle detekovány pomocí signatur, které jsou do aplikací integrovány prostřednictvím aktualizací. Tento klasický způsob detekce je navíc obvykle podpořen možností spolupráce s cloudem, obsahujícím rozsáhlejší databázi hrozeb. Z testovaných nástrojů využívá cloud vítěz testu Trend Micro, ale také nástroje od firem BitDefender a F- Secure.

V oblasti mobilního antivirového softwaru není problém falešných poplachů příliš aktuální, protože těch je u většiny nástrojů minimum. Abychom to ale otestovali, nechali jsme nástroje prověřit 487 aplikací, o kterých jsme stoprocentně věděli, že jsou „čisté". Zajímavé je, že v této oblasti se náš vítěz testu ocitl v nelichotivé společnosti posledního umístěného – nástroje od společnosti AegisLab, který také vyprodukoval jeden planý poplach.

Jako dobrou zprávu lze označit fakt, že stále více bezpečnostních aplikací nabízí kromě ochrany před instalací malwaru také ochranu v reálném čase. Ta se hodí například při surfování, kdy je uživatel upozorněn na hrozbu na navštívené WWW stránce nebo na phishingový útok. Ochranu při surfování tak nenajdete jen u produktů MicroWorld, Comodo, Eset, Sophos a AegisLab.

Zatížení systému

V rámci našeho testu bezpečnostních skenerů pro smartphony a tablety jsme ale nehodnotili jen jejich schopnost detekce hrozeb. Dalším ostře sledovaným parametrem byla zátěž systému. Ve srovnání se stolním počítačem totiž nenabízejí mobilní zařízení takový přebytek výkonu a jakákoliv zbytečná zátěž je na nich skutečně znát. Navíc každé další procento zátěže spotřebovává cennou energii a zkracuje dobu provozu na baterie.

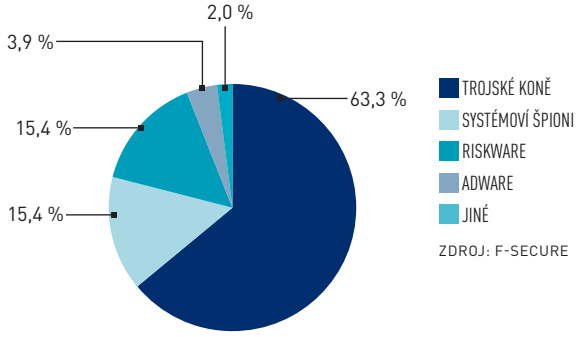
Naštěstí jsou si tohoto faktu vědomi i výrobci bezpečnostních řešení, a i přesto, že jejich software běží neustále na pozadí, až na jedinou výjimku nespotřebovávají příliš mnoho energie. Tou výjimkou je nástroj od AegisLab, který zpomaloval systém skutečně citelně a také podstatně zkracoval dobu výdrže na baterii. Všechny ostatní nástroje zatěžovaly procesor přibližně na úrovni jednoho či dvou procent.

CHIP BEZPEČNOSTNÍ SITUACE

Čím populárnější jsou smartphony, tím atraktivnějším terčem se stávají pro kyberzločince. Odborníci již dlouho považují OS Android za nová mobilní „Windows": tato platforma je jednoznačně nejrozšířenější, a proto v ní hackeři hledají (a bohužel nacházejí) bezpečnostní mezery.

NEJČASTĚJŠÍ VIRY PRO ZAŘÍZENÍ S OS ANDROID

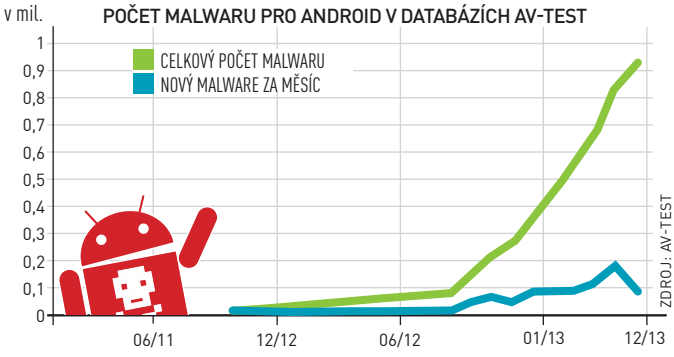
Přibližně dvě třetiny aktivních instalací malwaru pro Android tvoří trojské koně. Ty jsou obvykle skryty v neškodných aplikacích a jejich cílem je tajně posílat drahé prémium SMS. Systémoví špioni jsou méně rozšíření, i když i jejich obliba mezi hackery stoupá. Tyto nástroje prohledávají zařízení a hledají o něm a jeho uživateli informace.



ZDROJ: F-SECURE

PRUDKÝ NÁRŮST ŠKODLIVÉHO SOFTWARU PRO ANDROID

Viry pro Android se šíří stále rychleji. V posledních několika měsících bezpečnostní experti z organizace AV-Test detekovali až 200 000 nových variant virů měsíčně. Celkový počet aktivních hrozeb pro tuto platformu se blíží k jednomu milionu.



ZDROJ: AV-TEST

POUŽÍVÁNÍ INTERNETU NA MOBILNÍCH ZAŘÍZENÍCH

Jak tento graf ukazuje, aktivní surfování po webu se pomalu přesouvá na mobilní zařízení. V současné době nejsou žádné útoky škodlivého softwaru zahájeny prostřednictvím webových stránek pro mobilní zařízení, odborníci však předpokládají, že taktika „drive-by download" bude nakonec pro mobilní zařízení představovat hrozbu, stejně jako je tomu u klasických prohlížečů.

ZDROJ: BLUECOAT

Když je výbava zklamáním...

Ačkoliv na nás mobilní antiviry zapůsobily minimální zátěží systému a zčásti i svými detekčními schopnostmi, přesto jsme u nich narazili na oblast, kde nás vyloženě zklamaly. Z hlediska výbavy totiž žádná z bezpečnostních aplikací nenabídla všechny funkce, které jsme od programů tohoto typu očekávali.

Dobrou zprávou tedy alespoň je, že všechny aplikace, včetně té od AegisLab, to myslí s ochranou dat na ztraceném zařízení zcela vážně. Uživatelé mohou na dálku ztracený přístroj lokalizovat, zamknout, nebo z něj dokonce odstranit soukromá data. Pro operace tohoto druhu se obvykle používá jeden ze dvou různých přístupů. První z nich využívá SMS příkazů, zatímco druhý zahrnuje využití webových stránek. Například v případě nástrojů Kaspersky nebo Avast (nejlepší free aplikace) mohou uživatelé používat pro ovládání ztraceného smartphonu SMS příkazy, zatímco v případě aplikací od BitDefenderu a Trend Micro můžete totéž provést pomocí webových stránek. Obě metody umožňují dosáhnout stejného výsledku, podle našeho názoru je ale práce pomocí WWW stránek praktičtější.

Naopak nepříliš spokojeni jsme byli v oblasti šifrování, kde naše očekávání na sto procent nesplnila žádná z aplikací, pouze zčásti pak aplikace od firmy Sophos. Podle našeho názoru je problém v tom, že výrobci spoléhají na implicitní funkci OS Android, která ale není ani příliš známá, ani příliš oblíbená.

Zcela zklamáni jsme byli z hlediska zálohovacích funkcí, kde body ztratila většina aplikací. Jedinými výjimkami, kterým záleží i na bezpečnosti vašich dat, jsou nástroje od MicroWorld, McAfee, Comodo, G-Data a Lookout. Velkým překvapením pro nás také bylo, že jen u tří nástrojů z celého testu nechyběla dětská pojistka.

Naše očekávání se tak naplnila alespoň v oblasti blokování nechtěné komunikace. Většina bezpečnostních aplikací totiž nabízí blokování hovorů a SMS zpráv.

Jednoduché ovládání

Ovládání mobilních bezpečnostních aplikací je mnohem snazší, než je tomu u klasických virových skenerů pro Windows. Důvodem je pochopitelně i fakt, že mobilní aplikace mají mnohem méně funkcí a možností nastavení. Na druhé straně je ale nutné přiznat, že pokud jde o návrh rozhraní a výchozí nastavení, odvedli výrobci velmi dobrou práci.

To ale bohužel neznamená, že bychom k rozhraní aplikací neměli vůbec žádné výtky. Nelíbilo se nám, že až na výjimky většina aplikací není vybavena stavovým displejem, který označuje, zda je vše v pořádku. Tuto funkci nabízí vítěz testu Trend Micro Mobile Security a některé aplikace, jako například Kaspersky, poskytují informace pouze na hlavní obrazovce.

Líbilo se nám, že všechny funkce těchto aplikací jsou přístupné přes centrální obrazovku. Neexistuje tedy žádné riziko, že by vaší pozornosti uniklo důležité nastavení skryté v podnabídce.

Během testu jsme byli také ohromeni výchozím nastavením výrobce – i bez složité konfigurace vždy všechno fungovalo bez problémů. Nicméně i zde byly mezi jednotlivými nástroji drobné rozdíly. Zatímco například u vítěze testu Trend Micro se během skenování zobrazil jednoduchý ukazatel procentuálního stavu operace, u některé konkurence (například Comodo a F-Secure) tato funkce citelně chyběla. Ta totiž dává uživatelům přibližnou představu o tom, jak dlouho bude tento otravný proces trvat.

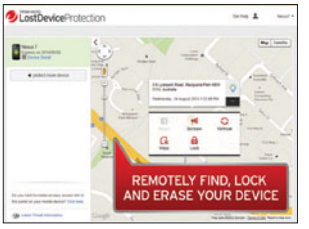
I přes zmiňované výtky jsme byli celkově spokojeni. Většina mobilních aplikací splnila svůj úkol (ochranu před malwarem) na jedničku a překážkou pro uživatele by neměla být ani cena.

DŮLEŽITÉ DOPLŇKY V BEZPEČNOSTNÍCH APLIKACÍCH

Přestože se diskuse při výběru antiviru často točí kolem detekce virů, trojských koní a dalších forem škodlivého softwaru, měl by i jednoduchý antivirový software nabídnout další vlastnosti. Za klíčové považujeme především tyto:

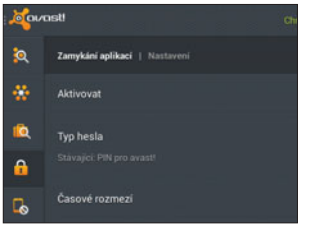
NALEZENÍ ZTRACENÉHO TELEFONU

Byl váš smartphone odcizen nebo ztracen? Pokud ano, můžete k jeho nalezení použít bezpečnostní aplikaci. To lze provést dvěma různými způsoby. Zařízení můžete sledovat a ovládat pomocí speciálních SMS nebo ho můžete vyhledat pomocí webové stránky. Druhá varianta je obvykle jednodušší.



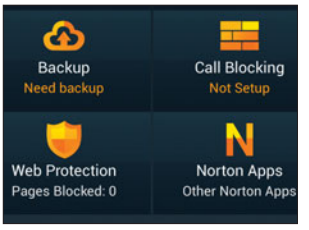
ZAMYKÁNÍ PŘÍSTROJE A ODSTRANĚNÍ DAT

Pokud se váš smartphone již dostal do rukou někoho jiného, měli byste zabránit zneužití na něm uložených dat. První krok spočívá v uzamčení zařízení tak, aby žádná neoprávněná osoba nemohla prohlížet vaše kontakty, fotografie a další data.



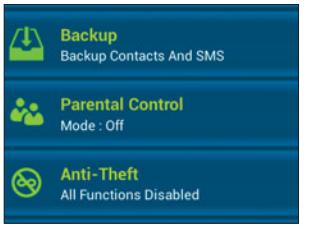
ZÁLOHA OSOBNÍCH ÚDAJŮ

Přibližně třetina z testovaných aplikací nabízí i zálohovací funkci – jako například Comodo. Váš mobilní telefon s OS Android je ale možné zazálohovat pomocí jiných nástrojů, jako je třeba Ultimate Backup Tool.



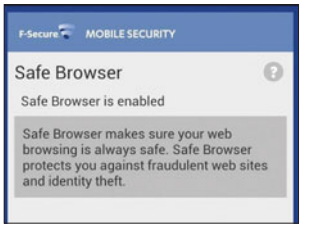
RODIČOVSKÝ ZÁMEK

Nezávisle na tom, zda jde o tablet či chytrý telefon, ochrana „před dětmi" se vždycky hodí. A to jak možnost zakázat instalaci pochybných aplikací, tak i například filtrování navštěvovaných webů.



OCHRANA PŘI SURFOVÁNÍ

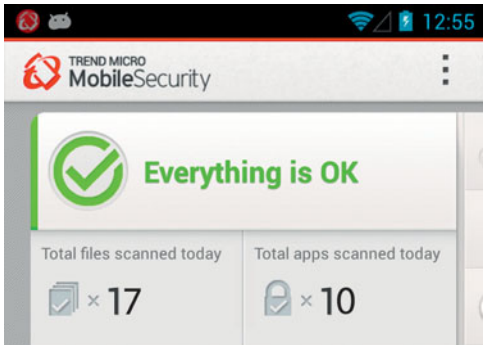
Všechny testované aplikace zvládají detekci virů, ale jen některé z nich jsou vybaveny automatickou ochrannou funkcí při surfování. Tato funkce je obzvláště důležitá v případě, že uživatel používá mobilní zařízení především na surfování a na internetu tráví dlouhou dobu. Funkce chrání uživatele zejména před kontaminovanými webovými stránkami a phishingovými útoky.



ŠIFROVÁNÍ

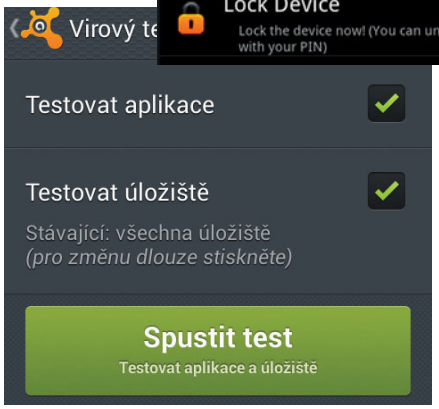
OS Android nyní dokáže šifrovat data i bez pomoci dalších aplikací, mnoho uživatelů však tuto funkci nezná. Přesto se může šifrování v bezpečnostní aplikaci hodit i proto, že obvykle nabízí mnohem více funkcí a možností nastavení.

PLACENÁ INZERCE



Vítěz testu: Trend Micro boduje nejlepšími detekčními schopnostmi a výbavou.

Žádné skutečné slabiny: Třetí místo obsadil nástroj McAfee Mobile Security.



Dokáže toho hodně a nic nestojí: Avast! Mobile Security.

Ochrana proti krádeži je stejně důležitá jako antivirová ochrana

Virová zkušební laboratoř AV-Test podrobila bezpečnostní aplikace pro Android také vytrvalostní zkoušce. Chip získal podrobné výsledky za posledních šest měsíců. Z hlediska hodnocení schopnosti detekce byly použity viry, které byly shromážděny v průběhu roku 2013. Testovacím OS byl Android 4.2.2. Aby byl scénář co nejrealističtější, mohly aplikace používat připojení k internetu a aktualizovat se automaticky. Díky tomu měly antiviry s mechanismem rychlých aktualizací výhodu nad ostatními.

Detekční schopnost (25 %): Bylo zkontrolováno 2 545 malwarových aplikací, které byly organizací AV-Test shromážděny během čtyřtýdenní přípravy na test.

Zatížení systému (25 %): Testovali jsme vliv fungování bezpečnostního softwaru na životnost baterie, zda zpomaluje další aplikace a případně i datový provoz.

Výbava (25 %): V této oblasti získávaly antivirové programy důležité body za zálohovací nástroje, možnost šifrování nebo schopnost lokalizovat, zamknout a vymazat data ze ztraceného zařízení.

Ovládání (25 %): Hodnotíme především logiku ovládání, od instalace až k nastavení detailů.

CHIP VÝSLEDKY TESTU

Dobrá antivirová ochrana pro OS Android nemusí stát nic. Mezi deseti nejlepšími aplikacemi ve srovnávacím testu lze najít i dvě aplikace, které jsou k dispozici zdarma, a to !Avast Mobile Security a Comodo Mobile Security & Antivirus Free. Vítěze testu, Trend Micro Mobile Security, je však možné získat pouze za peníze – tedy konkrétně za roční poplatek asi 20 eur. Spolu s působivou úrovní detekčních schopností antiviru tento produkt nabízí, ve srovnání s dalšími testovanými aplikacemi, také nejlepší výbavu a nejpříjemnější ovládání.

Pokud chcete trochu ušetřit, můžete zvolit nástroj od F-Secure, který (kromě horšího ovládání) nabízí podobnou úroveň bezpečnostních funkcí, a to za roční poplatek 15 eur. Aplikace na druhém a třetím místě také nabízí dobrou úroveň zabezpečení, jejich cena je však podle našeho názoru příliš vysoká. Skromnější uživatelé ale mohou zvolit například i bezplatnou aplikaci od Avastu, která také poskytuje účinnou ochranu pro smartphony i tablety...

Vítěz testu: S velmi působivou schopností detekce a nejlepší úrovní ovládání nabízí Trend Micro Mobile Security nejlepší poměr mezi cenou a výkonem. Jediným bodem kritiky tak může být skutečnost, že jako jedna z mála testovaných aplikací měla i falešný poplach.

Cenový tip: Pokud jde o bezplatné bezpečnostní aplikace, v této oblasti je Avast nesporným vítězem. Jeho čtvrté místo v testu dokazuje, že dobrá ochrana nemusí stát nic. Další bezplatná aplikace, Comodo, je také vhodná pro detekci virů, zaostává ale v oblasti komfortu ovládání a také nabídka doplňkových funkcí je slabá.

ANTIVIROVÉ SKENERY PRO ANDROID

Pořadí	Produkt	Celkové hodnocení	Cena za rok	Od Androidu verze	Detekce (25 %)	Zatížení systému (25 %)	Výbava (25 %)	Ovládání (25 %)	Úroveň detekce (procent)	Falešné poplachy	Možnost lokalizace	Zamknutí	Smazání	Blokování hovorů	Filtr zpráv	Ochrana surfování	Dětský zámek	Zálohování	Šifrování
1	Trend Micro Mobile Security	92,4	19,95 euro	2.2	100	100	77	93	99,9	1	•	•	•	•	•	•	•	–	–
2	MicroWorld eScan Mobile Security	91,9	30,89 euro	2.2	100	100	77	91	99,9	0	•	•	•	•	•	•	–	•	–
3	McAfee Mobile Security	91,3	29,99 euro	2.1	97	100	77	91	99,4	0	•	•	•	•	•	•	–	•	–
4	avast Mobile Security & Antivirus	89,3	zdarma	2.1	99	100	66	92	99,8	0	•	•	•	•	•	•	–	–	–
5	Symantec Norton Mobile Security	89,3	29,99 euro	2.1	99	100	66	92	99,8	0	•	•	•	•	•	•	–	–	–
6	F-Secure Mobile Security	88,9	14,95 euro	2.2	97	100	77	82	99,3	0	•	•	•	•	•	•	•	–	–
7	Kaspersky Mobile Security	88,1	10,95 euro	2.2	97	100	66	90	99,3	0	•	•	•	•	•	•	–	–	–
8	Comodo Mobile Security & Antivirus Free	88,0	zdarma	2.2	99	100	66	87	99,8	0	•	•	•	•	•	–	–	•	–
9	G Data MobileSecurity 2	87,5	18,99 euro	2.1	83	100	77	90	96,6	1	•	•	•	•	•	•	–	•	–
10	Dr. Web Antivirus	86,6	9,90 euro	v závislosti na zařízení	93	100	66	88	98,5	0	•	•	•	•	•	•	–	–	–
11	Eset Mobile Security	85,6	14,83 euro	2.0.1	98	100	55	89	99,7	0	•	•	•	•	•	–	–	–	–
12	Lookout Security & Antivirus	83,5	35,88 euro	v závislosti na zařízení	89	100	55	90	97,8	0	•	•	•	–	–	•	–	•	–
13	Bitdefender Mobile Security	82,3	8,99 euro	v závislosti na zařízení	100	100	44	85	100	0	•	•	•	–	–	•	–	–	–
14	Sophos Mobile Security	79,0	zdarma	2.2	90	100	44	82	98,0	0	•	•	•	–	–	–	–	–	•
15	AegisLab Antivirus Free	34,5	zdarma	2.1	10	33	10	85	58,1	1	–	–	–	–	–	–	–	–	–