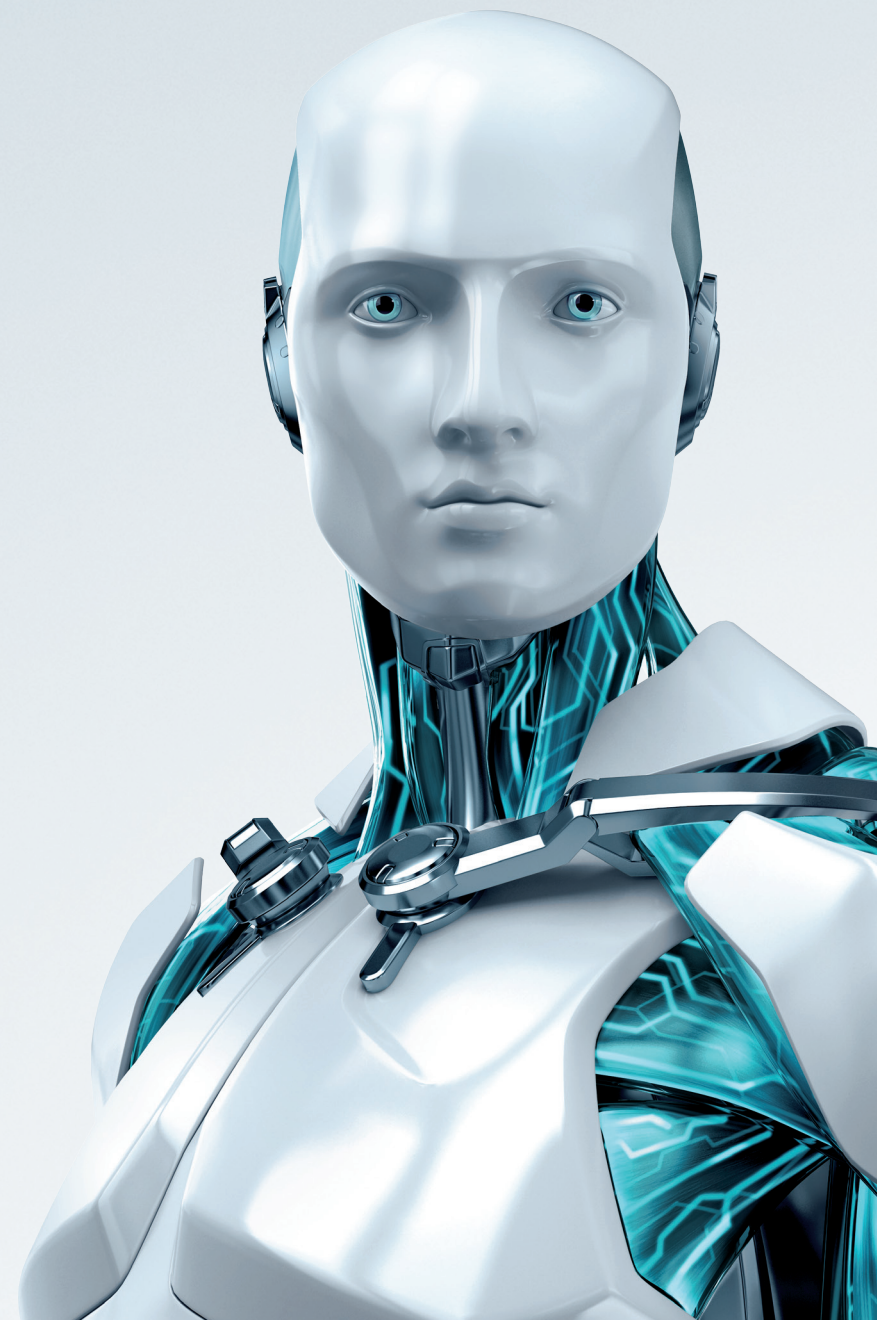


Trójsky kôň Boxer SMS

Hrozba útočiaca na Android
smartfóny v 63 krajinách

André Goujon, Pablo Ramos, výskumníci spoločnosti ESET



Úvod

Výskumný tím ESETu v Latinskej Amerike sa rozhodol analyzovať trójskeho koňa Boxer navrhnutého pre platformu Android po tom, čo sa nám s problémom ozvalo niekoľko užívateľov. Tím zistil, že hrozba, ktorú ESET Mobile Security identifikuje ako Android/TrojanSMS.Boxer.AA¹, sa zameriava na viac ako 60 krajín.

Po tom, čo sme vzorku analyzovali a jej správanie vyhodnotili ako SMS trójskeho koňa, ktorý používa príkazy na odosielanie SMS správ na spoplatnené čísla, sme dokázali taktiež identifikovať internetových užívateľov, ktorým sa na faktúrach od mobilných operátorov objavili záhadné poplatky.

Táto štúdia vysvetľuje charakter hrozby, technické charakteristiky škodlivého kódu a spôsob, akým zasiahol obyvateľov až 60 krajín.

SMS trójske kone

SMS trójsky kôň je kategória škodlivého kódu pre mobilné telefóny, ktorého hlavným cieľom je prihlásiť obeť k odberu spoplatnených SMS služieb. Keďže tento typ služby väčšinou užívateľa informuje o úspešnom prihlásení k odberu, niektoré trójske kone tejto kategórie preto filtrujú SMS správy z týchto spoplatnených čísel tak, aby užívateľ o tejto infekcii nevedel. To znamená, že vidí len štandardné SMS správy a nie správy prijaté z týchto spoplatnených čísel. Pre užívateľa to znamená závažný finančný problém: ak si neskontroluje stav svojho mobilného účtu, počká si naňho vysoká faktúra. Diagram na nasledujúcej strane znázorňuje správanie SMS trójskeho koňa. Ako je vidieť, užívateľ spustí škodlivú aplikáciu, ktorá odošle SMS správu. Následkom toho je útok týmto škodlivým kódom vytvoreným špeciálne pre mobilné prístroje, ktorý útočníkovi generuje profit.

¹ http://www.virus-radar.com/en/Android_TrojanSMS.Boxer.AA/description



Škodlivý kód

Vo všeobecnosti majú SMS trójske kone limitovaný dosah, sú napríklad schopné zasiahnuť len konkrétne krajiny, keďže telefónne čísla spoplatnených služieb sú v rôznych krajinách odlišné a môžu sa líšiť aj v prípade rôznych operátorov. Napriek tomu má Boxer dosah na 63 krajín v Amerike, Európe, Afrike, Ázii a Oceánii. To z neho robí SMS trójskeho koňa s vysokým potenciálom pre šírenie po veľkom geografickom území (presné dôvody vymedzenia tohto územia nie sú známe avšak zrejme sa mal zamerať na krajiny, v ktorých by dokázal užívateľom ukradnúť viac peňazí).

Infekcia a jej šírenie

Keďže Boxer je trójskym koňom, nedokáže sa šíriť sám. Z toho dôvodu ho musia ľudia stojaci za touto hrozbou uploadovať na webstránku alebo úložisko. Okrem toho tiež využívajú techniky sociálneho inžinierstva na to, aby potenciálnu obeť zmanipulovali k tomu, aby malware (škodlivý kód) spustila.

V decembri 2011 bolo v digitálnej službe Google Play (bývalý Android Market) nájdených 22 aplikácií infikovaných touto hrozbou². Na infikovanie týmto malwarom boli využívané aplikácie ako Sim City Deluxe Free, Need for Speed Shift Free, Assassin Creed a niektoré doplnky pre Angry Birds. Tieto infikované aplikácie boli z Google Play už dávno odstránené, hlavným šíriteľom tejto nákazy na Android smartfónoch sú neoficiálne stránky a úložiská. Z tohto dôvodu by nebolo prekvapivé, ak by tento trójsky kôň získaval nové obeť práve cez tento typ webstránok.

2 <http://blogs.eset-la.com/laboratorio/2011/12/15/limpieza-android-market/>

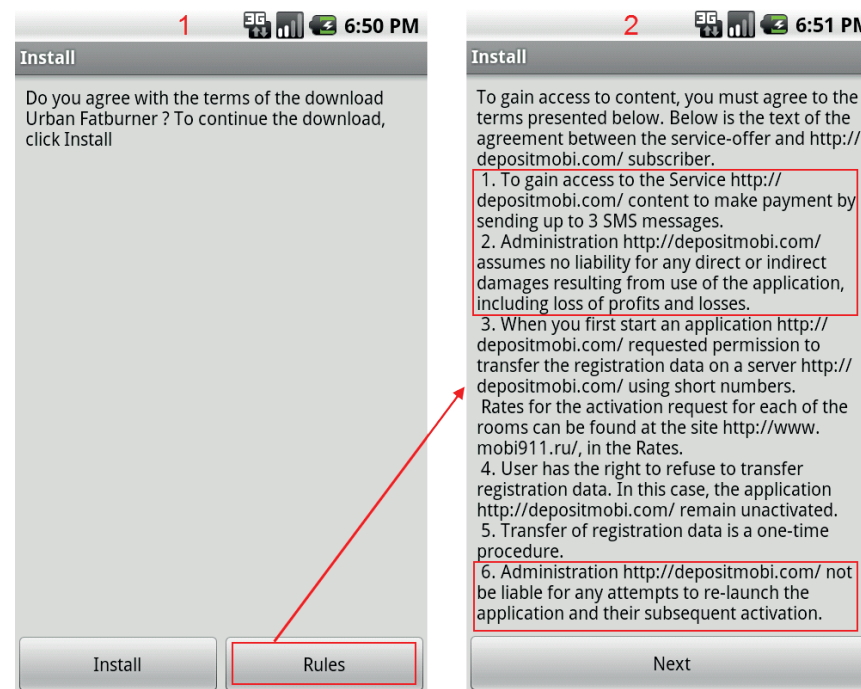
Android/TrojanSMS.Boxer.AA

Pre účel tejto analýzy sme použili vzorku identifikovanú ako Android/TrojanSMS.Boxer.AA, ktorú sme našli v aplikácii určenej na meranie spaľovania tuku „Urban Fatburner“ (Md5: 962078fba0bca8cda4fe39c516d21ffc). Ak si chce užívateľ stiahnuť a nainštalovať tento škodlivý softvér, musí dať aplikácii povolenia na vykonávanie týchto úkonov:

- Odosielanie textových správ
- Prijímanie textových správ
- Uskutočňovanie telefonických hovorov
- Prijímanie WAP PUSH
- Prístup k internetu

Ak by si užívateľ všimol všetky povolenia vyžadované aplikáciou, uvedomil by si toto podozrivé správanie aplikácie, keďže aplikácia určená na meranie spáleného tuku by na svoju činnosť nepotrebovala prijímať alebo odosielať SMS správy. Pred ukončením inštalácie sa užívateľovi zobrazí súhlas s používaním licencie v ktorom je napísané, že užívateľ môže byť prihlásený k odberu spoplatnených SMS správ. Niektoré informácie však v licencii chýbajú. Napríklad to, že užívateľovi budú pravidelne odosielať spoplatnené správy. Tvorcovia tejto hrozby zneužili fakt, že takmer nikto nečíta licenciu pri inštalácii softvéru. Dva obrázky znázorňujú Android systém (verzia 2.3), ktorý je práve infikovaný: Prvý zobrazuje informáciu, ktorú užívateľ uvidí pri spustení Boxera. Druhý ukazuje časť súhlasu s používaním licencie SMS trójskeho koňa. Táto informácia sa však zobrazí až po stlačení tlačidla Rules/Pravidlá.

Ak by bol človek dostatočne obozretný a prečítal by si súhlas s využívaním licencie, všimol by si jeho podozrivé časti ako napríklad obmedzenú zodpovednosť providera v prípade, že využívaním aplikácie dôjde užívateľ k priamym alebo nepriamym škodám (bod 2).



Taktiež by si mohol všimnúť chýbajúce spoplatnené čísla a poplatok za ich využívanie. V bode 1 sa píše, že pre prístup k obsahu musí aplikácia odoslať menej než tri alebo práve tri správy. Bod 6 však hovorí o tom, že pri nasledujúcom spustení aplikácie môže opätovne dôjsť k jej aktivácii. To znamená, že užívateľ bude musieť pri každom spustení tejto aplikácie a zároveň hrozby platiť za niekoľko spoplatnených SMS správ. Legitímna aplikácia by samozrejme nemala byť aktivovaná viac než jeden krát.

Payload: Prihlásenie k odberu spoplatnených SMS správ

Ak užívateľ akceptuje súhlas s používaním licencie, trójsky kôň začne zisťovať identifikačné číselné kódy podľa krajiny a operátora MCC (Mobile Country Code = mobilný kód krajiny) a MNC (Mobile Network Code = kód mobilnej siete). Týmto spôsobom zistí, v ktorej krajine sa telefón nachádza a služby ktorého operátora využíva. Následne začne odosielať správy na spoplatnené čísla, ktoré vydedukoval zo získaných informácií. Analýza trójskeho koňa nám umožnila identifikovať časti kódu, v ktorom sú uložené MCC kódy. Tieto kódy sú neskôr využité pre identifikáciu krajiny, v ktorej sa smartfón nachádza:

```
private static final String ARAVIA_MCC = "420";  
private static final String ARGENTINA_MCC = "722";  
private static final String ARMENIA_MCC = "283";  
private static final String AVSTRIA_MCC = "232";  
private static final String AZ_MCC = "400";  
private static final String BELGIA_MCC = "206";  
private static final String BELORUS_MCC = "257";  
private static final String BOLGARIA_MCC = "284";  
private static final String BOSNIAGERC_MCC = "218";  
private static final String BRAZILIA_MCC = "724";  
private static final String CHEHIA_MCC = "230";  
private static final String CHERNOGORIA_MCC = "297";  
private static final String CHILI_MCC = "730";
```

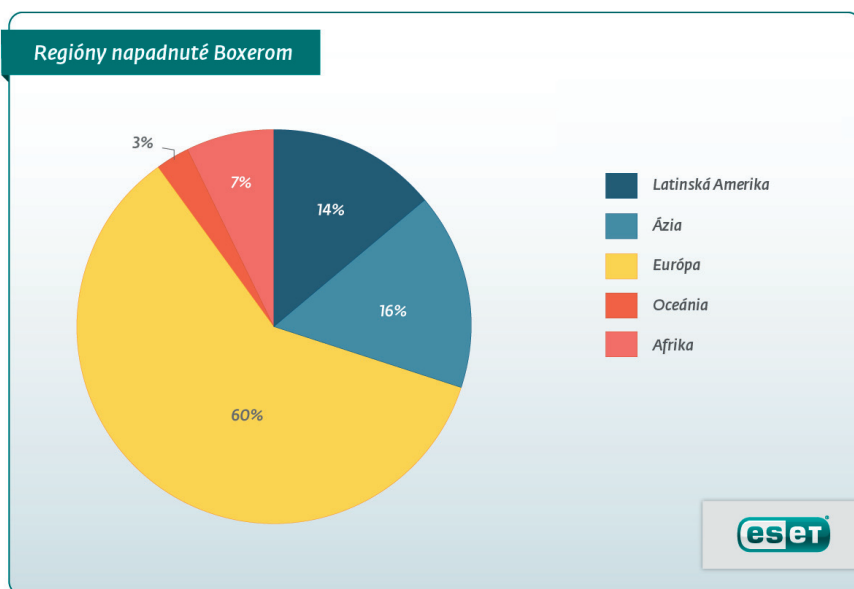
Škodlivý kód obsahuje 63 MCC kódov asociovaných s krajinami v rôznych kútoch sveta. Túto informáciu Boxer používa na určenie telefónneho čísla, na ktoré odošle SMS správu pre prihlásenie sa k prístupu k spoplatneným službám.

Keď Boxer identifikuje krajinu v ktorej sa nachádza, aktivuje v smartfóne aktuálnu inštaláciu čo znamená, že na spoplatnené čísla odošle niekoľko textových správ so všetkými informáciami, ktoré kyberkriminálni potrebovali na získanie finančného obnosu.

Svetový dopad

Počas analýzy sme sa zamerali na dopad, ktorý mal tento SMS trójsky kód v Latinskej Amerike, keďže sme mali prístup k sťažnostiam dotknutých užívateľov v tomto regióne. Nič menej, zo 63 napadnutých krajín bolo 60 percent v Európe, 16 v Ázii, 14 percent v Severnej a Latinskej Amerike, sedem percent v Afrike a tri percentá v Oceánii.

Napadnuté spektrum krajín je široké a môže nás viesť k ďalšej analýze toho, ako by mohlo byť toto prostredie zdrojom zárobku pre kyberkriminalnikov. Ako sme už informovali³, trh, ktorý platí kriminálnikom za každú jednu inštaláciu malwaru (Pay Per Install) na mobilné zariadenie rastie. Boxer je jednou z viac rozšírených hrozieb, ktorá na zisk peňazí používa tento obchodný model. Medzi najviac zasiahnuté časti Európy patria Rusko, Francúzsko, Nemecko, Česká republika a Poľsko. Celosvetovú distribúciu tohto malwaru znázorňuje táto mapa:



³ <http://blog.eset.com/2012/09/12/dancing-penguins-a-case-of-organized-android-pay-per-install>

Kompletný zoznam 63 krajín, ktoré zasiahol trójsky kôň SMS Boxer

Európa	Litva	Ukrajina	Ázia
Arménsko	Lotyšsko	Veľká Británia	Hong Kong
Azerbajdžan	Luxembursko	Amerika	Izrael & Palestína
Belgicko	Maďarsko	Argentína	Jordánsko
Bielorusko	Moldarvsko	Brazília	Kambodža
Bosna a Hercegovina	Nemecko	Čile	Katar
Bulharsko	Nórsko	Guatemala	Kirgizsko
Cyprus	Poľsko	Honduras	Libanon
Česká republika	Portugalsko	Mexiko	Malajzia
Čierna Hora	Rakúsko	Nikaragua	Saudská Arábia
Dánsko	Rumunsko	Panama	Spojené arabské emiráty
Estónsko	Rusko	Peru	Taiwan
Fínsko	Slovinsko	Afrika	Oceánia
Francúzsko	Srbsko	Alžírsko	Nový Zéland
Grécko	Španielsko	Egypt	
Holandsko	Švajčiarsko	Juhoafrická republika	
Chorvátsko	Švédsko	Macedónsko	
Kazachstan	Turecko	Maroko	

Vo svete sa objavili aj novšie varianty tejto hrozby a zoznam krajín, na ktoré sa zamerali, už nie je taký dlhý. Niektoré krajiny z neho boli vyškrtnuté zrejme pre nízke príjmy alebo pre problémy s platbou. Varianta, ktorú sme analyzovali, bola súčasťou 22 aplikácií v digitálnej službe Google Play, čo zvyšovalo šancu, že si ju nainštaluje veľké množstvo užívateľov. Po tom, čo Google tieto aplikácie zo služby vymazal, objavil sa Boxer v internetových úschovniach. V tomto prípade už nebolo nutné zamerať sa na vysoký počet krajín, keďže odsunutím aplikácií s malwarom do úschovni sa výrazne znižuje ich šanca na úspešnú inštaláciu.

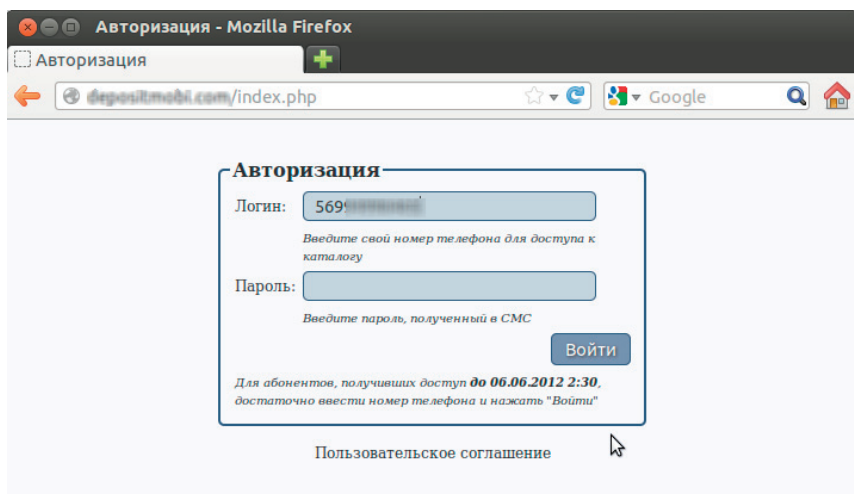
Viac informácií

Okrem prihlásenia užívateľa na prístup k spoplatneným SMS službám sa Boxer pokúša o pripojenie k dvom webstránkam. Prvá je ESET produktmi zablokovaná od septembra 2011, keďže je spojená s iným malwarom vytvoreným pre mobilné zariadenia: J2ME/TrojanSMS.Konov.AB. Stránka po načítaní zobrazí políčka, do ktorých môže užívateľ vpísať svoje telefónne číslo. Informácie uložené v škodlivom súbore budú neskôr použité na prihlásenie infikovaného smartfónu k spoplatneným SMS službám. Užívateľovi sa však nezobrazí informácia, ako by mohol používanie tejto služby ukončiť. Ak obeť nie sú schopné túto službu deaktivovať, ich účet za využívanie spoplatnených správ stále rastie.

Android/TrojanSMS.Boxer.AA



Sú nám známe správy o tom, že za každú jednu inštaláciu na Android prístroj získal kyberkriminalník 2-5 dolárov. V prípade Boxera sa zdá, že so škodlivými aktivitami tohto malwaru je prepojená táto ruská webstránka:



Následne sa pokúša pripojiť k ďalšej webstránke. V čase analyzovania kódu a písania tejto štúdie bola táto druhá stránka offline. Z toho dôvodu sme nedokázali určiť jej obsah. Malware sa pokúša pripojiť aj k tretej webstránke, ktorej adresa je uvedená v sms.cfg súbore, ktorá je taktiež nedostupná.

Záver

Smartfóny sa pre ľudí stávajú stále viac prístupnými a populárnymi zariadeniami. Užívatelia si však pri mnohých príležitostiach nie sú vedomí hrozieb, ktorým môžu čeliť, ak neuplatnia preventívne bezpečnostné opatrenia. Na svete existujú SMS trójske kone

vytvorené aj pre iné platformy ako napríklad Symbian alebo pre mobilné zariadenia kompatibilné s Java Micro Edition. V roku 2012 sme však boli svedkom nárastu počtu takýchto hrozieb vytvorených špeciálne pre platformu Android, príkladom čoho je aj Boxer. Vo všeobecnosti útočia SMS trójske kone na veľmi malý počet krajín. Existujú prípady, kedy sú schopné vykrádať užívateľov vo viacerých krajinách jedného kontinentu, napríklad v Európe. Boxer je však schopný prekonať túto bariéru tak, že útočí v 63 krajinách na niekoľkých svetadieloch. Ak vezmeme do úvahy, že sme túto hrozbu našli v niekoľkých škodlivých aplikáciách na Google Play, z Boxera sa stal jeden z najvýznamnejších SMS trójskych koní tohto roka a je zároveň prvým, ktorý sa snaží útočiť v tak veľkom počte krajín.

Toto taktiež potvrdzuje hypotézu, že kyberkriminalníci nevyužívajú svoje zdroje len na tvorbu stále komplexnejšieho malwaru pre mobilné zariadenia ale aj na koncentrovanie svojich zdrojov na rozširovanie geografickej pôsobnosti malwaru. Je pravdepodobné, že v blízkej budúcnosti uvidíme viac škodlivého kódu zameraného na Android prístroje a zároveň vyrobeného tak, aby zasiahol čo najviac regiónov vo svete.

Na záver je dôležité spomenúť, že pre zníženie rizika inštalácie malwaru sú potrebné jednoduché úkony ako napríklad prečítanie súhlasu využívania licencie pri inštalácii aplikácie. Ak ste sa vy alebo niekto vo vašom okolí stretli s nevysvetliteľnými poplatkami za mobilný telefón, skontrolujte svoj prístroj na prítomnosť škodlivého kódu.