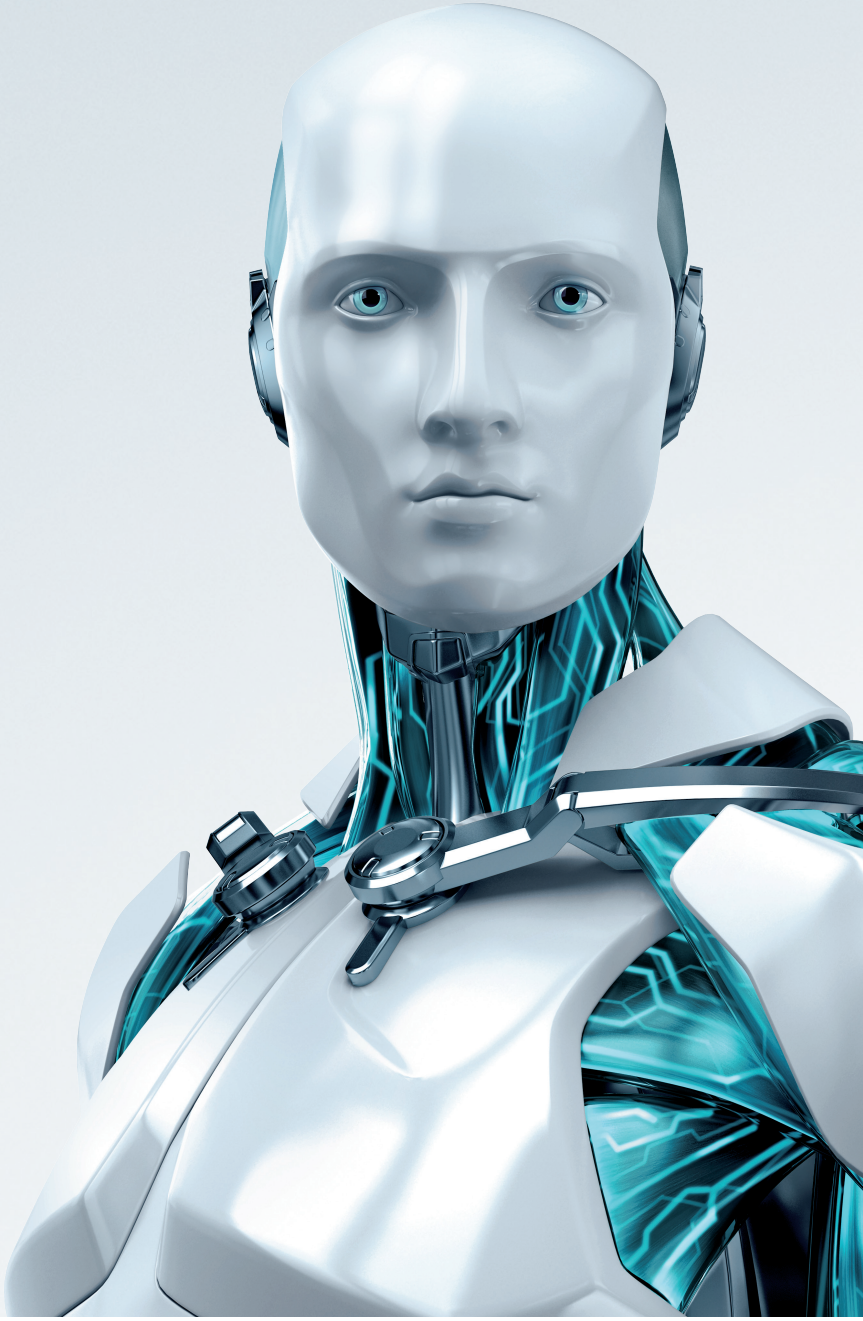
Kybernetické hrozby v roku 2013

Mohutný rast mobilného malwaru

Výskumné laboratórium ESET Latinská Amerika



Úvod

Na konci každého roka pripravuje latinskoamerické laboratórium spoločnosti ESET správu o trendoch vývoja malwaru, kybernetického zločinu a iných typoch škodlivých útokov. Je založená na tom, čo bolo analyzované a zaznamenané v priebehu aktuálneho roka. Je dôležité poukázať na to, že trendom myslíme odhad vykonaný spoločnosťou na základe aktuálneho stavu výskytu dátových hrozieb a kybernetického zločinu.

Trendy vývoja malwaru sa menili aj počas písania týchto správ. Napríklad hlavným trendom pre rok 2010 bolo „**Dozrievanie crimewaru**", pre rok 2011 to boli „**Botnety a dynamický malware**" a pre rok 2012 zase „**Malware sa zmobilnieva**". Všetky tieto témy majú niečo spoločné a za každou sa skrýva honba kyberkriminálnikov za finančným ziskom. Je preto celkom pozoruhodné, ak jediný trend prechádza takým rýchlym rastom počas tak krátkeho času, ako sa stalo v prípade fenoménu mobilného malwaru.

V priebehu roka 2012 sme boli schopní sledovať, ako sa škodlivé programy vytvorené pre operačný systém Android zmenili na významný nástroj kyberkriminálnikov, ktorí začali malware zameraný na tieto zariadenia vytvárať oveľa rýchlejšie.

Počas prvého štvrťroka 2012 zaznamenal operačný systém spoločnosti Google podľa IDC medziročný rast 145 percent, čo sa týka predaja a podielu na trhu[1]. Juniper Research okrem toho predpokladá, že počet ľudí, ktorí sa k svojim bankovým službám prihlasujú cez svoj smartfón vzrastie v roku 2013 na 530 miliónov[2]. Tá istá štúdia hovorí, že v roku 2011 to bolo len 300 miliónov ľudí. V kontexte rastu predaja, širokých možností využitia a vzhľadom na rapídnu evolúciu ako tejto technológie tak i škodlivých programov vytvorených pre mobilné prístroje si myslíme, že **hlavným trendom roku 2013 bude exponenciálny rast mobilného malwaru**. Taktiež predpokladáme, že tieto hrozby naberú na komplexnosti, čo znamená, že **rozšíria škálu škodlivých úkonov, ktoré na infikovanom zariadení vykonajú**.

V roku 2013 tiež očakávame konsolidáciu zmeny, ktorá prebieha posledných niekoľko rokov: je ňou zmena modelu, ktorým kyberkriminálnici propagujú/šíria škodlivý kód. Šírenie malwaru pomocou vymeniteľných médií ustupuje pred šírením cez medzičlánok, ktorý má pritiahnuť nové obete. Medzičlánkom je web server, ktorý bol skompromitovaný treťou stranou na to, aby mohol hostiť počítačové hrozby. Po napadnutí servera rozosielajú kyberkriminálnici užívateľom hyperlinky, ktoré ich navedú k škodlivému softvéru. V tom istom čase sú ukradnuté údaje ukladané na napadnutých serveroch. Ak by sa totiž ukladali do počítačov užívateľov, ktoré môžu byť proti útokom lepšie chránené, mohli by po náleze a vyčistení malwaru kriminálnici o tieto nakradnuté údaje prísť.

Keď vezmeme všetky tieto informácie do úvahy, s akými trendmi sa stretneme v nasledujúcom roku 2013? Účelom tejto štúdie je poskytnúť

1 Smartfóny s Androidom a iOS zvýšili podľa IDC v prvom štvrťroku 2012 svoj podiel: http://www.idc.com/getdoc.jsp?containerId=prUS23503312

2 Štúdia Juniper Research: Banking Anytime Anywhere: http://www.juniperresearch.com/whitepapers/anytime_anywhere

vysvetlenia a odpovede na túto otázku tak, aby mohli korporátni i domáci užívatelia prijať vhodné opatrenia, ak chcú byť náležite chránení pred najnovšími hrozbami.

Významný nárast mobilného malwaru

Od roku 2010 začal trh i technológie mobilného malwaru prechádzať veľkými zmenami, ktoré začali meniť následnú evolúciu tohto druhu hrozby. V prvom rade sa začal Android na trhu pozicionovať ako najpopulárnejší mobilný operačný systém. V tom istom roku sa stal *Fake Player* prvým malwarom, ktorý sa zameral na Google platformu. Následne v roku 2011 výskumné laboratórium ESETu v Latinskej Amerike predpovedalo, že sa v priebehu roka tento mobilný operačný systém stane platformou, na ktorú sa tvorcovia malwaru zamerajú najviac... čo sa následne aj potvrdilo.

O rok neskôr nevzrástla len frekvencia v ktorej bol pre Android vytváraný škodlivý kód a jeho varianty, ale aj jeho komplexnosť a čo viac aj čas a zdroje, ktoré kyberkriminálnici zasvätili vývoju malwaru pre mobily. Je len logické, že operačný systém s 64,1-percentným podielom na trhu bude pre kriminálnikov tak atraktívny, keďže v tomto prípade budú mať väčšiu šancu nezákonne sa obohatiť než by mali v prípade operačného systému, ktorý by mal menší podiel užívateľov.

Diagram znázorňuje mobilné operačné systémy a ich aktuálny podiel na trhu:

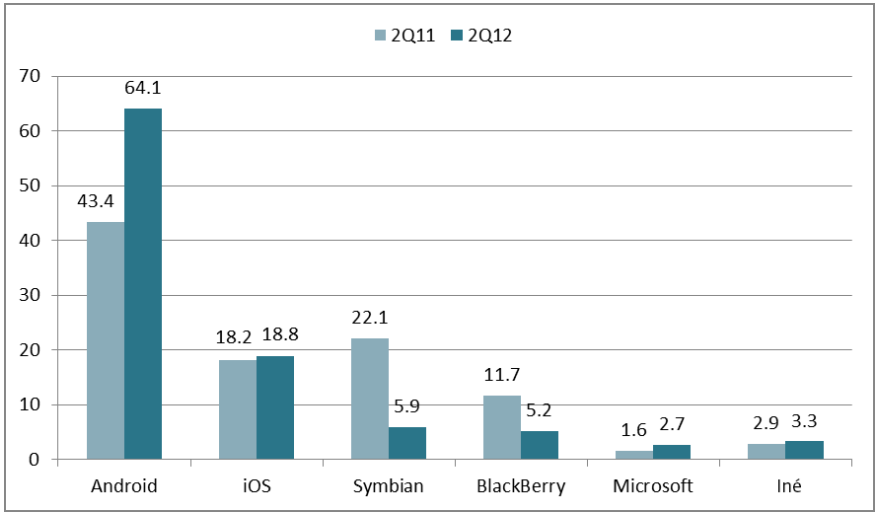


Diagram 1: Predaj smartfónov koncovým zákazníkom podľa operačného systému v druhom polroku 2012, Gartner: http://www.gartner.com/it/page.jsp?id=2120015.

Z diagramu je vidieť, že v porovnaní s rovnakým obdobím minulého roka (druhý kvartál 2011) zaznamenal Android nárast o 20,7 percenta, iOS (Apple) o 0,6 percenta a Microsoft o 1,1 percenta. Iné operačné systémy zaznamenali v porovnaní s rokom 2011 pokles v predaji. Najväčší pád zažil Symbian (16,2 percenta), nasledovaný BlackBerry s 6,5 percentami.

Keďže trhový podiel Androidu rastie a ľudia ho používajú stále viac a viac ako úložisko osobných i firemných údajov alebo na online bankovníctvo a podobné služby, budú kyberkriminálnici na kradnutie informácií vyvíjať viac malwaru, čo im pomôže generovať nezákonný zisk.

Ako je pre malware útočiaci na počítače bežné, hlavným motívom kyberkriminálnika pri vytváraní tohto druhu hrozby je ešte stále finančný zisk. Toto potvrdil aj objav prípadu „**Dancing Penguins**“. Ide o obchodný plán, v ktorom kyberkriminálnici použili nelegálny model Pay Per Install (PPI, platba za každú inštaláciu), v ktorom si za každú inštaláciu malwaru na Android prístroj vyžiadali 2-5 dolárov.

Podľa prieskumu, ktorý uskutočnil ESET Latinská Amerika a ktorý sa venoval **využívaniu mobilných prístrojov**, sme zistili, že osobné údaje a heslá nepredstavujú primárny typ informácie, ktorý užívatelia do smartfónu ukladajú. Z celého koláča uložených údajov však predstavujú významnú časť. Údaje z prieskumu znázorňuje tento graf:

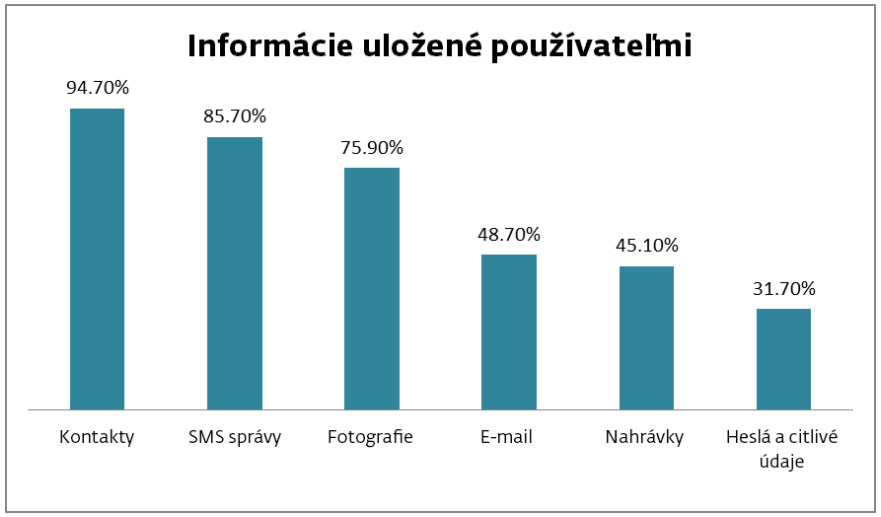


Diagram 2: Informácie uložené užívateľmi na mobilných zariadeniach

Ako je z grafu vidno, užívatelia si do týchto prístrojov najčastejšie ukladajú kontakty. Preto nie je žiadnym prekvapením, že existuje škodlivé kód pre Androidy vytvorený na kradnutie týchto dát. Kradnutie kontaktných údajov je spôsob, ktorým kriminálnici hľadajú nové obete. **Heslá a osobné informácie predstavujú 31,7 percenta uložených údajov**. Toto percento ešte vzrastie postupom času, v ktorom sa bude technológia smartfónov vyvíjať.

Nárast detekcie Android malwaru

Prvým štatistickým údajom, ktorý znázorňuje závratný nárast mobilného malwaru – údaj, ktorý nám umožňuje určiť, že trendom v roku 2013 bude exponenciálny nárast Android malwaru – je fakt, že **objem unikátnych vzoriek vzrástol celosvetovo počas roka 2012 v porovnaní s rokom 2011 až 17 krát**. Medzi krajinami, ktoré zažili v násobkoch najvyšší nárast je Ukrajina so 78-násobným vzrastom počtu vzoriek, Rusko so 65-násobným nárastom a Irán so 48-násobným nárastom. Ak by sme však počet vzoriek neporovnávali s predchádzajúcim rokom, krajinami s najvyšším počtom detekcií v roku 2012 by boli Čína, Rusko a Irán. Na základe týchto údajov teda môžeme prehlásiť, že počet vzoriek Android malwaru narastie v roku 2013 ešte viac.

Čo sa týka počtu malware rodín pre Android – to znamená škodlivých kódov, ktoré sú od seba dostatočne odlišné na to, aby mohli byť unikátne klasifikované – v minulom roku bolo do novembra detegovaných 52 rodín, v tomto roku bolo do novembra detegovaných už 56 rodín.

Napriek tomu, že toto číslo počas roka 2012 dramaticky nevzrástlo, tento dokument neskôr ukáže, že **počet signatúr a variánt vzrástol**

významne. Z toho dôvodu predpokladáme, že **počet Android hrozieb bude rásť bez ohľadu na počet malware rodín**. Podobne ako je tomu v prípade operačného systému Windows. Je dôležité pripomenúť, že pre kyberkriminálnika je jednoduchšie modifikovať už existujúci škodlivý kód (variantu), než napísať úplne nový kód. Nasledujúci obrázok znázorňuje rodiny malwaru zoskupené podľa roku a mesiaca, v ktorom boli objavené.

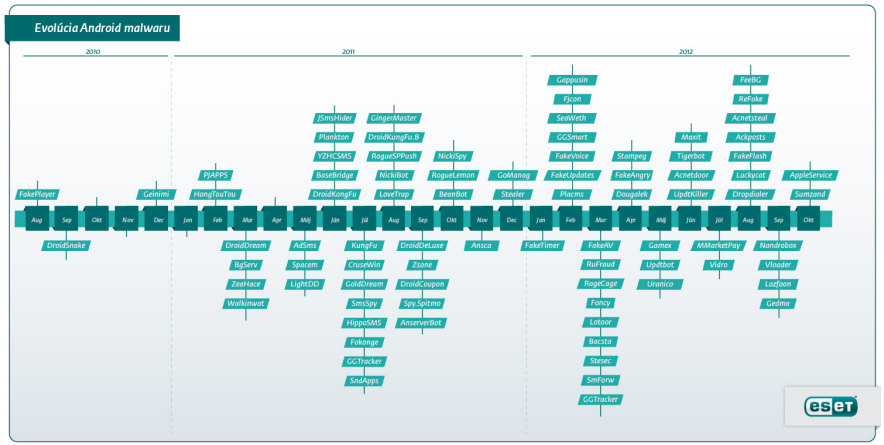


Diagram 3: Vznik rodín malwaru pre Android

Na základe rodín zobrazených v obrázku a škodlivej činnosti (payloadu) vykonanej na androidových zariadeniach môžeme klasifikovať ich správanie nasledovne: krádež informácií (spyware), distribúcia SMS správ na spoplatnené čísla a transformácia týchto zariadení na zombie zariadenia (získavanie botnetov). Na základe toho získame tento diagram:

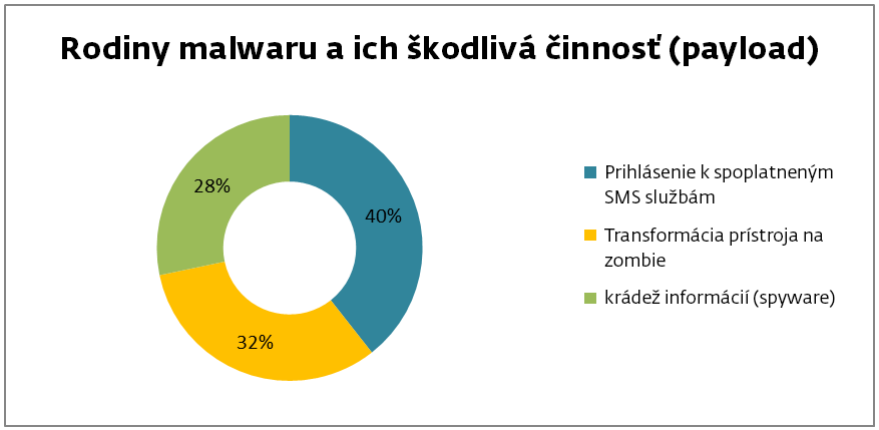


Diagram 4: Malware rodiny v roku 2010, 2011 and 2012 a ich škodlivá činnosť

Väčšina týchto rodín chce obeť prihlásiť k spoplatneným SMS službám. Na druhej strane existujú hrozby, ktoré dokážu tieto prístroje transformovať na zombíkov. To znamená, že prístroj bude môcť ovládať kyberkriminálnik, ktorý naň bude môcť vzdialene inštalovať ďalší škodlivý kód, bude z neho môcť kradnúť údaje a okrem iného bude môcť modifikovať konfiguračné parametre. V tretej skupine sú škodlivé programy, ktoré kradnú údaje ako telefónne čísla, SMS správy a ďalšie informácie, ktoré telefón dokážu identifikovať. Ide napríklad aj o IMEI číslo.

Na rozdiel od malwaru, ktorý transformuje smartfón na zombíka, kradne iný malware informácie aj bez toho, že by predal celú kontrolu prístroja do rúk kyberkriminálnikovi. Nakoniec existujú aj špeciálne prípady ako *Android/Stampeg*, ktorého úlohou je vložiť k JPG súborom

uloženým v smartfóne špeciálny obrázok, čo môže viesť k zlyhaniu pamäťovej karty. *Android/MMarketPay* zase dokáže sťahovať spoplatnené aplikácie z čínskeho online obchodu bez súhlasu užívateľa a *Android/FakeFlash* predstiera, že je Flash pluginom, užívateľa však presmerováva na konkrétnu webstránku.

Významný nárast variánt

Počet variánt Android malwaru vzrástol v priebehu roka 2012 tiež. Varianta je modifikovaná verzia špecifického a známeho škodlivého programu. Kyberkriminálnici modifikujú štruktúru a kód existujúcej hrozby na to, aby vytvorili novú hrozbu s pridanými novými škodlivými funkciami a aby sa zároveň zatajili pred antivírusovými programami. Diagram na tejto strane znázorňuje štyri malware rodiny a počet ich variánt, ktoré sa objavili v rokoch 2011 a 2012. ESET priraďuje každej novej významnejšej variante príponu v abecednom poradí. Napríklad prvá verzia hypotetického škodlivého programu sa bude volať *Hrozba.A* a druhá významnejšia varianta dostane názov *Hrozba.B*. Ak počet variánt prekročí číslo 26, čiže počet písmen v anglickej abecede, prípony nasledujúcich variánt sú podobným modelom rozšírené o ďalšie písmená: .AA, .AB,... .AAA, .AAB a tak ďalej.

Tento zjednodušený model sa však v niektorých špeciálnych prípadoch nedá použiť. Taktiež sa toto názvoslovie nedá považovať za spoľahlivú pomôcku, pretože jednotliví výrobcovia antivírusových programov môžu varianty pomenovávať odlišne.

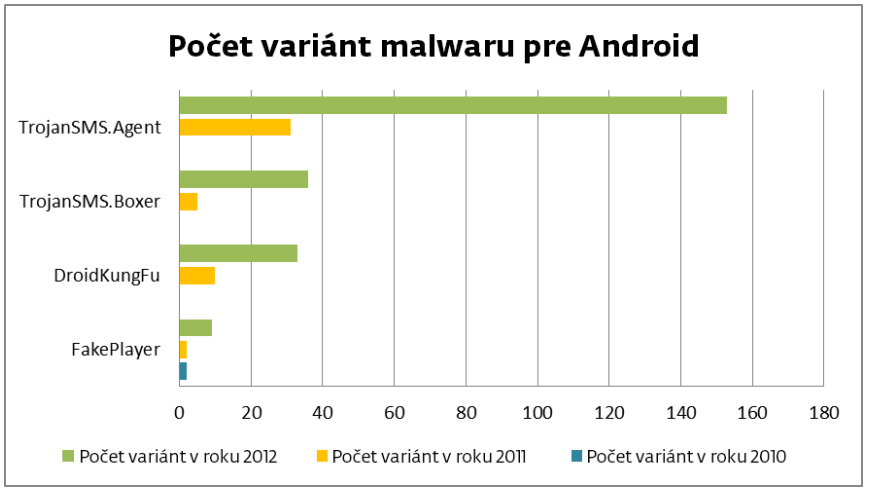


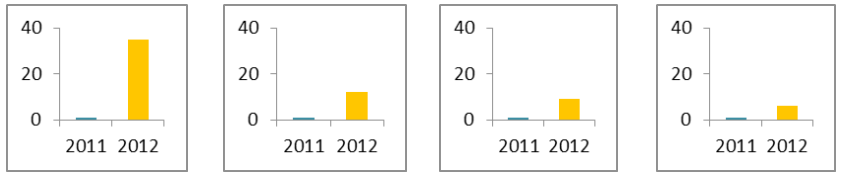
Diagram 5: Počet variánt malwaru pre Android

Ako znázorňuje diagram, najväčší rast v roku 2012 v porovnaní s rokom 2011 zaznamenal *TrojanSMS.Agent*. Zodpovedá plodnej rodine malwaru, ktorej členovia sú si vzájomne odlišní avšak majú jeden spoločný zámer: prihlásiť obeť k spoplatneným SMS službám. V roku 2011 mala rodina len 31 nových variánt, v roku 2012 však toto číslo narástlo na 153. Druhým v poradí je ďalší SMS trójsky kôň známy ako *Boxer*. Tento malware a niektoré z jeho osobitých vlastností budú vysvetlené na nasledujúcich stranách tejto štúdie, je však vhodné všimnúť si, že v roku 2011 sa táto rodina skladala z piatich variánt. V súčasnosti však ich počet narástol na 36. Podobný rast sme zaznamenali pri *DroidKungFu*: 10 variánt v roku 2011 a 33 v roku 2012. Na koniec tu máme *FakePlayer*, prvý malware zameraný na Android. V roku 2010 sa objavili dve varianty, rovnako tomu bolo aj v roku 2011, rok 2012 nám však priniesol deväť variánt.

Vyšší počet signatúr pre detekciu mobilného malwaru

Počet signatúr vyvinutých ESETom na detekciu škodlivého kódu vytvoreného pre Android v roku 2012 tiež značne narástol. Dôvodom je hore opísaný dramatický nárast variánt malwaru. Tabuľka 1 zobrazuje štyri rodiny s korešpondujúcimi údajmi. Pri každej reprezentuje žltá farba nárast v roku 2012 a modrá farba nárast v roku 2011. Je dôležité spomenúť, že signatúra je segment kódu, ktorý sa zameriava na detekciu jednej alebo viacerých hrozieb, preto ak počet signatúr narastie, je to z dôvodu potreby detekcie nového škodlivého kódu, ktorý sa objavuje na dennej báze. Počet signatúr však nie je priamoúmerný počtu variánt, a už vôbec nie počtu jedinečných binárnych súborov, keďže jedna signatúra môže detegovať mnoho malých variánt.

Nárast počtu rodín podľa počtu signatúr pridaných v roku 2012

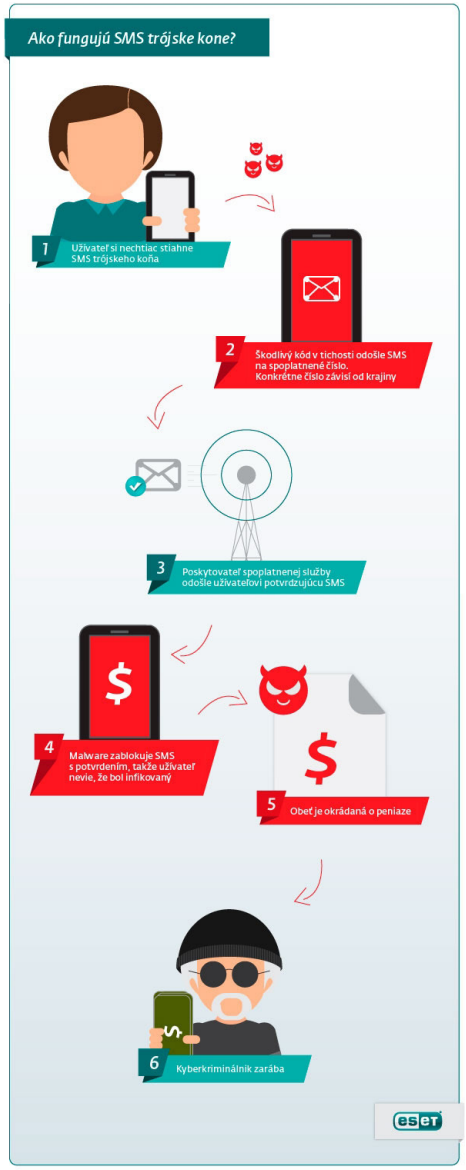


Plankton	JSmsHider	DroidDream	DroidKungFu
Počet signatúr vzrástol v roku 2012 35-násobne	Počet signatúr vzrástol v roku 2012 12-násobne	Počet signatúr vzrástol v roku 2012 9-násobne	Počet signatúr vzrástol v roku 2012 6-násobne

Žltá: 2012 | Modrá: 2011

Tabuľka 1: Nárast počtu rodín podľa počtu signatúr pridaných v roku 2012, verzus rok 2011

Podľa hornej tabuľky bol Plankton rodinou trójskych koňov s najvyšším rastom v roku 2012 a s najvyšším počtom signatúr nutných na detekciu všetkých svojich modifikácií. Počet signatúr na túto hrozbu vzrástol v porovnaní s rokom 2011 až 35-krát. Ďalšími v poradí sú *JSmsHider*, ktorého počty signatúr narástli 12-krát, *DroidDream* 9-krát a *DroidKungFu* 6-krát.



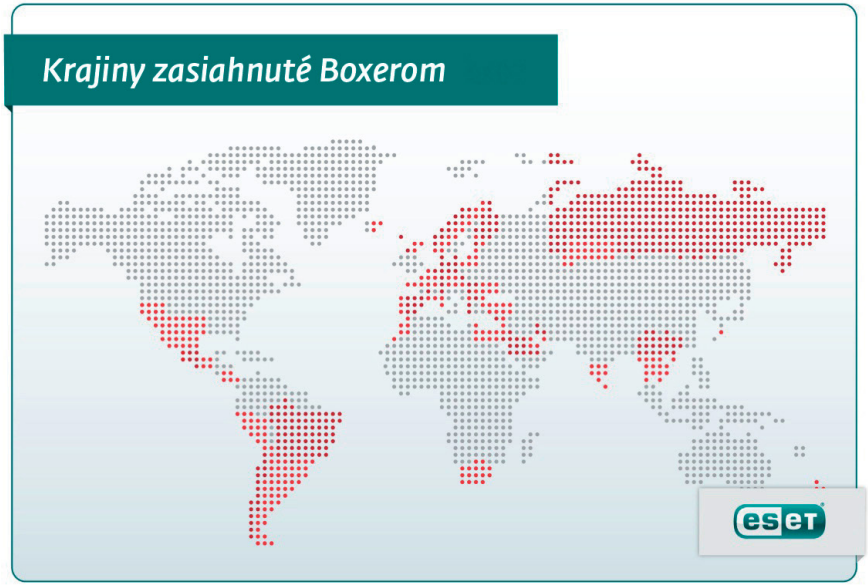
SMS trójany: najčastejšie hrozby pre smartfóny

SMS trójske kone sú najčastejšou hrozbou pre Android zariadenia. Najvyšší nárast, čo sa týka počtu variánt, zaznamenali len dve hrozby tohto druhu. Zoznamu jedinečných detekcií malwaru vytvoreného pre operačný systém od Googlu kraľoval v roku 2012 trójsky kôň *Android/TrojanSMS.Boxer.AQ*. Nasleduje ho *Android/Plankton.H* a *Android/TrojanSMS.Agent.BY.Gen*. Na tejto strane dokumentu je znázornené, ako tento typ mobilného malwaru zvyčajne funguje.

Pokiaľ budú kyberkriminálnici naďalej zarábať na tomto podvodnom obchodnom modeli a pokiaľ bude pre nich aj naďalej ľahko implementovateľný, je veľmi pravdepodobné, že SMS trójske kone budú aj v roku 2013 najrozšírenejšou mobilnou hrozbou.

Boxer: SMS trójan zameraný na 63 krajín

Ďalším míľnikom vo vývoji mobilného malwaru bol v roku 2012 objav varianty Boxera. *Boxer* je SMS trójan, ktorého hlavným cieľom je prihlásiť obeť k viacerým spoplatneným SMS službám tak, aby to kyberkriminálnikom generovalo nezákonný zisk. Táto hrozba má dve vlastnosti, ktoré ju odlišujú od iných podobných škodlivých programov. Prvou je, že **dokáže zasiahnuť 63 krajín**. Druhou je fakt, že bola nájdená **v 22 aplikáciách na Google Play**. Ak si užívateľ nedá pozor a jeho prístroj sa touto hrozbou infikuje, malware z telefónu zistí, v ktorej krajine sa nachádza a služby ktorého mobilného operátora využíva. Následne odošle tri SMS správy na spoplatnené čísla v danej krajine. Diagram znázorňuje krajiny zasiahnuté Boxerom:



Je bežné nájsť SMS trójske kone, ktoré sa zameriavajú na konkrétne krajiny alebo dokonca na špecifické regióny akými je napríklad východná Európa. Boxer sa však dokáže zamerať na Európu, Áziu a Ameriku. Je teda jedným zo škodlivých programov pre smartfóny s najväčším potenciálom na globálne šírenie, ktorý bol doteraz objavený.

O tomto malwari sa môžete dozvedieť viac v štúdii **Trójsky kôň Boxer SMS**[3].

Šírenie malwaru cez webstránky

Predstavenie prvej komerčnej verzie Windows XP v roku 2001 a masívne využívanie vymeniteľných médií odštartovali éru červov, ktoré sa šírili cez tieto médiá vďaka zneužitiu zraniteľnosti Windowsu XP (Autorun). Keďže tento **problém bol v roku 2009 vyriešený** a užívatelia premigrovali na novšie verzie Windowsu, počet škodlivých programov využívajúcich túto techniku v posledných rokoch ubudol (Je však dostatok malwaru, ktorý túto techniku stále obsahuje pre prípad, že natrafí na nezaplátaný systém).

Všetky detekcie spojené so zneužitím tejto výrobnej chyby (*INF/Autorun* a iné) v priebehu roka 2012 plynule klesali.

Na druhej strane generické detekcie ako *HTML/ScrInject.B*, *HTML/Iframe.B*, *JS/Iframe and JS/TrojanDownloader.Iframe.NKE* začali v **mesačnom rebríčku šírenia malwaru** okupovať druhú priečku a taktiež ďalšie miesta za ňou. Účelom týchto signatúr je detegovať rôzne webstránky, ktoré boli útočníkom skompromitované alebo modifikované tak, aby šírili malware. Vo väčšine prípadov ide o legitímne webstránky patriace rozličným spoločnostiam avšak kvôli zraniteľnosti, nedostatočnému zabezpečeniu alebo neadekvátnej konfigurácii boli modifikované kyberkriminálnikom, ktorému sa podarilo dostať sa na server, ktorý tieto webstránky hosťuje. Kyberkriminálnici potom do legitímnej stránky injektujú škodlivé skripty alebo iFramy: tieto presmerujú užívateľa na ďalšiu stránku, z ktorej si bude môcť stiahnuť hrozbu. V niektorých prípadoch sú tieto ukradnuté informácie taktiež uploadnuté na tento skompromitovaný server a nie na osobný počítač, aby útočník sťažil svoju identifikáciu.

Nasledovná tabuľka zobrazuje percentuálny nárast niektorých generických signatúr v roku 2011 a 2012, ktoré detegovali škodlivý kód šírený cez skompromitované webstránky a vymeniteľné médiá.

Signatúra	Percentuálny nárast v 2011	Percentuálny nárast v 2012	Trend pre 2013
INF/Autorun	5.8%	5.3%	↓
HTML/ScrInject.B	1.7%	4.3%	↑
JS/TrojanDownloader.Iframe.NKE	0.9%	1.2%	↑
JS/Iframe	0.6%	1.7%	↑
HTML/Iframe.B	1.5%	3.0%	↑

Tabuľka: Percentuálny nárast Autorun-u a signatúr, ktoré v roku 2011 a 2012 detegovali skompromitované webstránky

3 http://static1.esetstatic.com/fileadmin/Images/SK/Press/2012/2012-12-04/ESET-SMSBoxer-studia.pdf

V hornej tabuľke môžete vidieť, že v roku 2012 Autorun poklesol, zatiaľ čo iné signatúry súvisiace so skompromitovanými webstránkami narástli. Čísla korešpondujú s percentuálnym nárastom mesačných detekcií v každom roku. V niektorých prípadoch sme niektoré detekcie nezaznamenali v žiadnych mesiacoch roka.

Nasledovný diagram znázorňuje rok 2011 a časť roku 2012 – od januára po september. Ilustruje percento detekcií asociovaných s Autorun červami a hrozbami šírenými cez skompromitované web servery.

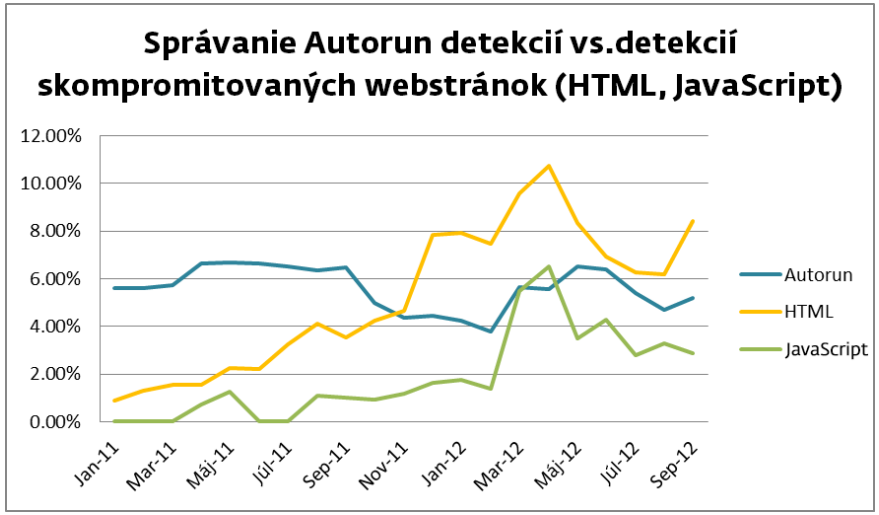


Diagram 6: Percento Autorun detekcií verzus detekcie skompromitovaných webstránok (2011 – september 2012)

Ako je vidieť, signatúry súvisiace so skompromitovanými webstránkami na začiatku roku 2011 takmer neexistovali. V priebehu roka začali Autorun detekcie klesať, v septembri ich predbehli HTML detekcie. Ba čo viac, ako HTML tak aj JavaScript zažili postupom času značný nárast. Toto nám dovoľuje konštatovať, že **druhým trendom v roku 2013 bude trvalý nárast využitia týchto techník za účelom infekcie potenciálnych obetí**. To znamená, že poklesne používanie červov zneužívajúcich vymeniteľné médiá.

Pred touto zmenou metód šírenia malwaru distribuovali kyberkriminálnici škodlivý kód do počítačov obetí rozličnými prostriedkami (e-mailom, sociálnymi sieťami, korporátnymi zdrojmi, vymeniteľnými médiami, atď.), ako zobrazuje nasledovný diagram:

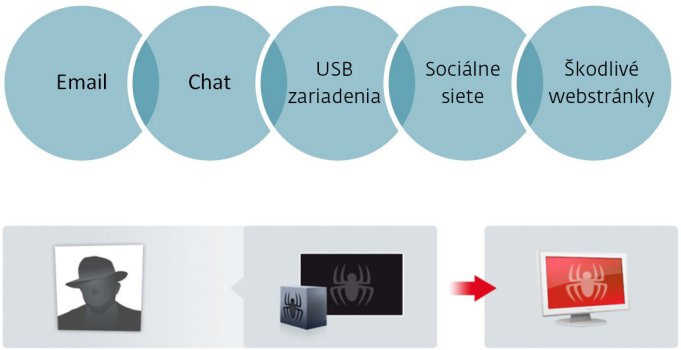


Diagram 7: Tradičná metóda šírenia malwaru

So zmenou v šírení malwaru, ktorá používa skompromitované webstránky, súvisí aj používanie medzičlánku (skompromitovaný server), ktorý kyberkriminálnikom tiež pomáha pri infekcii obete. Znázorňuje to tento diagram:

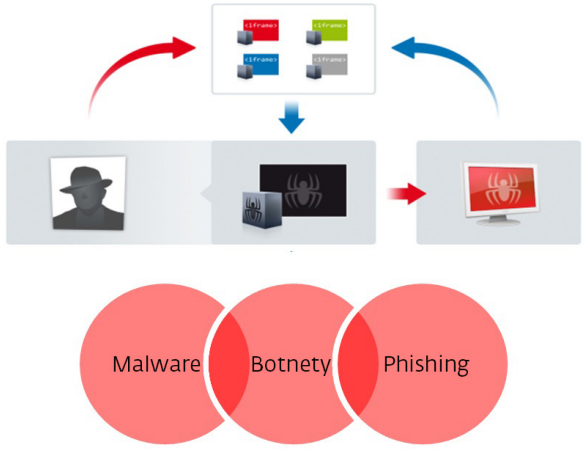


Diagram 8: Šírenie cez medzičlánok

Na to, aby mohol byť malware úspešne šírený cez webstránky, musí kyberkriminálnik uskutočniť nasledovné kroky:

1. Kyberkriminálnik zneužije existujúcu zraniteľnosť web servera. V ňom zmodifikuje originálnu stránku tak, že do nej injektuje škodlivý kód.

2. Začne šíriť link, ktorý užívateľov nasmeruje k hrozbe, ktorá sa nachádza na skompromitovanom servery. Hyperlink je zaslaný užívateľom cez e-mail, sociálne siete alebo ďalšími cestami.

3. Užívateľ navštívi túto webstránku a stiahne si malware. V niektorých prípadoch je informácia ukradnutá od obete na tomto medzičlánku (na servery) aj uložená.

Predtým, než sa tento trend etabloval, zvykli kyberkriminálnici celý tento proces preskočiť a malware šírili priamo k potenciálnym obetiam. Ukradnuté informácie zasielali a ukladali do svojich vlastných počítačoch.

Na druhej strane existuje okrem tejto techniky šírenia aj **Black Hat SEO**. Pri tejto technike používajú kybekriminálnici nezákonné metódy na to, aby škodlivé stránky umiestnili na horné priečky pri vyhľadávaní niektorých slovných reťazcov na internete. Vo väčšine prípadov používajú slovné reťazce, ktoré označujú nejakú tragédiu (buď takú, ktorá sa naozaj stala ale môže ísť aj o úplne vymyslené nešťastia) alebo populárne a známe osoby, ktorých mená slúžia na prilákanie potenciálnych obetí k tomu, aby si túto infikovanú stránku otvorili. Tieto phishingové útoky sú väčšinou uskutočnené cez medzičlánok a taktiež cez Command & Control (riadiace a kontrolné) centrá patriace do botnetu.

Botnety na vzostupe

Od roku 2010 si malware vytvorený na kradnutie informácií a generovanie zisku kyberkriminálnikom upevnil svoju pozíciu. V roku 2011 sme boli svedkom zreteľného nárastu týchto hrozieb a v roku 2012 pokračovali v stabilnom vzostupe. Červ ***Dorkbot*** je bezpochyby jednou z najúspešnejších hrozieb v regióne Latinskej Ameriky, počítač obete dokáže premeniť v zombíka. Príkladom toho, aký dosah mala táto hrozba je zistenie latinskoamerického výskumného laboratória ESETu, ktorý objavil botnet pozostávajúci z viac než 80-tisíc zombie počítačov, ktoré sa nachádzali hlavne v Čile (44 percent), Peru (15 percent) a v Argentíne (11 percent). *Dorkbot* sa šíril vďaka niekoľkým falošným spravodajským témam, ktoré vďaka sociálnemu inžinierstvu nalákali užívateľov na škodlivé stránky. Išlo napríklad o falošné videá, ktoré mali znázorňovať nehody Jennifer Lopez, Huga Cháveza, Lionela Messiho alebo Alexisa Sáncheza. Na šírenie použili jeho tvorcovia aj falošné súťaže s výhrami. Z technického hľadiska sa niektoré varianty tejto hrozby šírili cez vymeniteľné médiá, sociálne siete, Windows Live Messenger a cez ďalšie kanály. Táto hrozba okrem iného kradne citlivé údaje ako prístupové údaje k e-mailovým účtom a heslá.

V tomto konkrétnom prípade ESET zistil, že 88 percent ukradnutých e-mailových účtov patrilo firmám. Zvyšných 12 percent bolo zaregistrovaných v službách ako Gmail, Hotmail alebo Yahoo!. Diagram znázorňuje počet zombie počítačov (systémy infikované botom) a typ užívateľa podľa operačného systému.

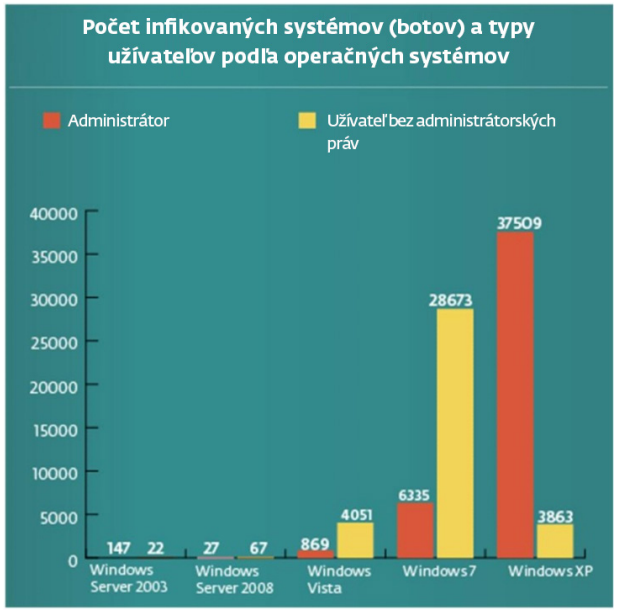


Diagram 9: Počet infikovaných systémov a typy užívateľov podľa operačného systému

Ako je vidno na diagrame, väčšina infikovaných užívateľov má ešte stále Windows XP a používa účet s administrátorskými právami. Napriek tomu, že táto hrozba je schopná bežať pod akýmkoľvek účtom, je dôležité, aby užívatelia pri bežnej práci robili pod prihlasovacími účtami so skresanými právami. Vďaka tomu sa niektorý škodlivý kód nebude môcť spustiť a ak sa mu to aj podarí, jeho funkcionalita bude obmedzená.

Ďalším malwarom s charakteristikami botnetu o ktorom sme informovali v roku 2012 je ***Flashback***. Väčšina malwaru tohto druhu je vyrobená pre Windowsy, tento trójsky kôň však zasiahol Mac OS X, operačný systém spoločnosti Apple. Podľa informácií zozbieraných spoločnosťou ESET dokázal **Flashback infikovať okolo 750-tisíc Mac užívateľov**. Tento prípad tiež ukazuje, že užívateľ by mal pri práci na počítači používať isté bezpečnostné návyky bez ohľadu na to, aký operačný systém používa. Očakávame, že počet botnetov v roku 2013 porastie, keďže kyberkriminálnikom dávajú do rúk flexibilný nástroj na generovanie nezákonného zisku zasielaním inštrukcií zombie systémom.

Cloud a prípady úniku informácií

Ukladanie dát v cloude je ďalším trendom, ktorý zaznamenal v roku 2012 nárast. Podľa spoločnosti Gartner[4], má rastúce používanie zariadení s kamerami, akými sú tablety alebo smartfóny, priamy vplyv na zvýšenú potrebu užívateľov ukladať viac údajov do cloudu. Je možné, že vplyv na nárast používania tejto technológie mali aj iné udalosti, ako napríklad záplavy, ktoré v prvej polovici roku 2012 zasiahli thajské továrne na výrobu hard diskov.

Predpokladom správy spoločnosti Gartner je, že v roku 2011 bolo v cloude uložených len 7 percent súborov od koncových užívateľov. Do roku 2016 však predpokladajú nárast na 36 percent. Táto technológia síce užívateľom uľahčuje prístup k informáciám z prakticky akéhokoľvek zariadenia s prístupom na internet, zároveň však z týchto zariadení robí objekt atraktívny pre tvorcov škodlivého kódu. To znamená, že sa tieto zariadenia stávajú náchylnejšie k útoku, ktorý dokáže skompromitovať údaje a vyvolať ich únik. Dôkazom toho bolo, keď útočníci získali prístup k niektorým ***Dropbox*** účtom. Prístupové údaje však získali z iného miesta. Toto teda nebola chyba služby Dropbox, naviedlo ju to však k tomu, aby zlepšila svoje zabezpečenie. Cloud teda nie je – rovnako ako počítačové systémy – bez bezpečnostných hrozieb. Je pravdepodobné, že čím viac využívanie tejto technológie porastie, tým viac sa o ňu začnú zaujímať kyberkriminálnici, aby mohli prostredníctvom nej generovať zisk.

Ďalšími portálmi, ktorým v roku 2012 unikli údaje, boli LinkedIn, Yahoo! a Formspring. Mainstreamové spoločnosti poskytujúce platobné a kreditné karty ako Visa a MasterCard museli vydať bezpečnostné varovania po tom, čo jeden platobný systém zaznamenal únik údajov. Tento incident sa dotkol 56 455 účtov patriacich obom spoločnostiam, 876 z nich bolo použitých na istú formu podvodu.

Hacktivizmus

V poslednej dobe bolo možné sledovať nárast protestov a demonštrácií obyvateľov rozličných krajín ako Grécko, Španielsko, Čile a Argentína. Protesty neobišli ani Slovensko. Dôvodom bola vždy nejaká sociálna alebo spoločenská nespokojnosť. Keďže technológie a svet počítačov sú súčasťou života mnohých ľudí, narástol aj aktivizmus využívajúci počítačové systémy (hacktivizmus). Na začiatku roka 2012 napadli členovia skupiny Anonymous niekoľko webstránok. Dôvodom bol ich hnev zo zatvorenia portálu Megaupload. Následkom toho spadla stránka FBI a na verejnosť preniklo niekoľko citlivých informácií o Robertovi Müllerovi, riaditeľovi tejto organizácie. Sony Music Entertainment sa tiež stal terčom útoku hacktivistov po tom, čo sa tá istá skupina rozhodla

4 Zdroj: http://www.gartner.com/it/page.jsp?id=2120015.

protestovať proti podpore legislatívnych zmien autorských práv. V tomto prípade získali Anonymous prístup k multimediálnym materiálom umelcov a tvorcov filmov, ktorých zastrešuje Sony, a následne ich zverejnili na internete.

V priebehu roka 2012 protestovali hacktivistické skupiny aj proti iným záležitostiam, útočili na webstránky patriace argentínskym, čilským, venezuelským a bolívijským subjektom. Vo väčšine prípadov bolo následkom útoku znefunkčnenie prístupu k obsahu stránky. V iných prípadoch využili útočníci techniku defacementu: na protest alebo pre výsmech modifikovali pôvodný obsah webstránky. Tiež sme sa stretli so správami, ktoré hovorili o útokoch s väčším dopadom: napríklad skupina AntiSec tvrdila, že sa dostala k 12 miliónom jedinečných identifikátorov (UDID) Apple produktov; počuli sme o vývoji linuxového operačného systému (Anonymous OS Live) s personalizovanými mechanizmami dovoľujúcimi uskutočnenie DDoS útoku; správy tiež hovorili o personalizovanom botnete nasmerovanom na webhostingovú spoločnosť GoDaddy alebo úniku informácií z 200-tisíc peruánskych domén, ktoré si na konto pripísala skupina Lulz Security Perú.

Z pohľadu dátovej bezpečnosti hacktivizmus dokázal, že organizácie majú v oblasti ochrany systémov na technologickej, administratívnej a výchovnej úrovni ešte stále čo robiť. Zo zapájania sa do netradičných protestov cez elektronické médiá sa stal rastúci trend. Ak majú ľudia sociálny problém, svoj názor naň už nevyjadrujú len tradičnou formou protestu. V roku 2013 sa veľmi pravdepodobne stretneme s touto netradičnou formou protestu v prípadoch, kedy bude pre ľudí pohodlnejšou voľbou práve kyberdemonštrácia.

Zraniteľnosti

Kyberkriminálnici odhaľujú zraniteľnosti z toho dôvodu, že im uľahčujú šírenie malwaru. Odhalenie zraniteľnosti dovoľuje spustiť škodlivý kód bez nutnosti zásahu užívateľa. Napríklad pri návšteve stránky s touto zraniteľnosťou je možné infikovať užívateľa bez toho, aby si stiahol a spustil program alebo hrozbu. Ako dôkaz môžeme spomenúť niektoré zraniteľnosti objavené v roku 2012. Trójsky kôň, ktorého bezpečnostné riešenia ESETu identifikovali ako *Win32/Poison* bol šírený vďaka zero-day zraniteľnosti platformy Java. Ak stránka obsahovala škodlivý applet, užívateľ sa ním nakazil len tým, že túto stránku navštívil. Problémom Javy a bezpečnostných narušení je to, že táto technológia pracuje na mnohých platformách. To znamená, že bezpečnostný problém by mohol mať za následok šírenie hrozby vytvorenej pre niekoľko operačných systémov. Ďalším softvérom zasiahnutým kritickou zraniteľnosťou bol Internet Explorer. Táto slabina umožnila kriminálnikom šíriť ďalšiu variantu červa Poison. Tieto problémy následne vyriešili obe spomenuté spoločnosti.

Na optimalizáciu týchto útokov vyvíjajú kyberkriminálnici bezpečnostné sady na zraniteľnosti, ktorých súčasťou je niekoľko bezpečnostných problémov a taktiež spôsoby, akými ich exploitovať. Napriek tomu, že tento trend nie je nový, najnovšia verzia (verzia 2.0) Blackholu – ide o známu expolitačnú sadu – dokazuje, že útočníci do nej aktívne dodávajú nové exploity a zraniteľnosti pre jednoduchšie šírenie malwaru. Novoobjavené bezpečnostné zraniteľnosti a metódy slúžiace na ich zneužitie budú optimalizované za účelom šírenia malwaru.

Ďalšou zraniteľnosťou, ktorá v roku 2012 vyčnievala nad ostatnými (a ktorá je istým spôsobom naviazaná na fenomén šírenia Android

malwaru), je objavenie bezpečnostnej chyby na niektorých prístrojoch s operačným systémom od spoločnosti Google, ktorá útočníkom umožňovala resetnúť prístroj na výrobné nastavenia, vďaka čomu mohli z telefónu alebo tabletu vymazať uložené údaje. Ak si užívateľ na prístroji otvorí škodlivú stránku, ktorá túto chybu zneužíva, útočník tým na prístroji vytočí sieťový kód (USSD číslo), čo môže mať za následok premazanie telefónu alebo tabletu. Ako formu ochrany je možné nainštalovať si zdarma **ESET USSD Control**. Tento nástroj je k dispozícii v digitálnej službe Google Play. Napriek tomu, že Android zraniteľnosti nie sú zneužívané tak často ako zraniteľnosti Windowsu, je možné, že kyberkriminálnici budú venovať hľadaniu týchto zraniteľností viac času za účelom finančného obohatenia sa.

Malware pre nové technológie

Vývojom technológií sa z pôvodne jednoduchých vynálezov akými sú televízia, automobily, routery a čipové karty stali prístroje s novými spôsobmi využitia komunikačných technológií. Niektoré televízie sa napríklad dokážu pripojiť k internetu a existujú taktiež automobily, ktoré majú v sebe implementovaný GPS systém, ktorý im pomáha pri hľadaní ciest a miest. Tieto inovácie dokážu život človeka zjednodušiť alebo obohatiť, kyberkriminálnikom však uľahčujú vývin malwaru, ktorý by tieto prístroje zneužíval.

Postupným vývojom zariadenia sa rozšíri jeho komplexnosť i funkcionalita, z toho dôvodu vzrastie pravdepodobnosť, že niekto vytvorí hrozbu, ktorá bude zneužívať chybu alebo zraniteľnosť tohto zariadenia. V súčasnosti napríklad ESETu deteguje malware útočiaci špeciálne na moderné televízory vyrábané známou kórejskou spoločnosťou. Trójsky kôň detegovaný ako *Perl/Agent.B* hľadá pripojenie k internetu. Ak ho nájde, divákovi ukáže správu o tom, že si musí nainštalovať aktualizáciu. Ak inštaláciu odsúhlasí, televízor sa vypne. Napriek tomu, že tento malware nespôsobuje žiadnu trvalú škodu a ani nekradne informácie tak dokazuje, že je možné vytvoriť hrozbu pre prístroje, ktoré nemusia byť počítačmi, tabletmi alebo smartfónmi.

Podobným prípadom bola hrozba detegovaná ako *Linux/Hydra.B*, o ktorej sme informovali v marci 2012. Je to škodlivý kód, ktorý sa pre zombie prístroje pokúša vytvoriť sieť. Na rozdiel od iného malwaru, ktorý sa pokúša vytvoriť botnet, sa Hydra zameriava na netradičné embednuté operačné systémy bežiace na IP priemyselných kamerách, domácich routeroch, VoIP (Voice over IP) systémoch, smartfónoch a tabletoch. V čase objavenia sa k riadiacemu a kontrolnému centru (Command & Control Center) prihlasovalo viac než 11-tisíc botov. Ukazuje to, že tomuto škodlivému kódu sa podarilo splniť svoj cieľ naverbovať netradičné zombie prístroje. Výskumník Paul Rascagneres zase hovoril o útoku založenom na škodlivom kóde, ktorého cieľom bolo umožniť vzdialený prístup k čipovým kartám. Výskum predstavený na bezpečnostnej konferencii Blackhat 2011 ukázal možnosť zásahu do bezpečnostného systému áut novej generácie. V konkrétnom prípade bolo možné automaticky odomknúť dvere auta a naštartovať motor pomocou bezdrôtovej technológie. Výrobca automobilu bol o tejto chybe informovaný, prezentácia bola však dôkazom, že aj táto technológia dokáže byť nabúrateľná.

Smartfóny sa do formy mini počítačov vyvinuli z jednoduchých mobilných telefónov, ktoré boli schopné uskutočniť telefonické hovory a odosielať SMS správy. Keďže iné prístroje prechádzajú podobným

evolučným procesom, budeme zrejme svedkom útokov nasmerovaných na tieto vynovené zariadenia. Problém sa zväčší ak do úvahy vezmeme, že Java platforma dokáže bežať na rozličných operačných systémoch. Ďalším faktom je, že je aj bez toho obľúbeným terčom kyberkriminálnikov.

Záver

Napriek tomu, že škodlivý kód vytvorený pre platformu Android bude hlavným trendom vo vývoji hrozieb v roku 2013, šírenie malwaru cez skompromitované webstránky bude taktiež naďalej rásť. Tradičný trh s počítačmi sa nevyvíja takou istou rýchlosťou ako predaj smartfónov, kyberkriminálnici budú však pokračovať vo vývoji veľkého množstva malwaru pre počítače.

Dokedy budú ľudia mohutne využívať počítače, budú na seba upriamovať záujem tvorcov počítačových hrozieb. Úloha užívateľov a komunity zostane teda nezmenená: na svojich mobilných zariadeniach a počítačoch používať nie len bezpečnostné riešenia ale sa aj oboznamovať s bezpečnostnými hrozbami, ktoré môžu na tieto zariadenia útočiť. Napriek tomu, že dokážu život človeka uľahčiť, môžu v prípade nesprávneho zaobchádzania predstavovať vážny problém pri zabezpečení digitálnej identity užívateľa.