BANKOVNÍ TROJSKÉ KONĚ

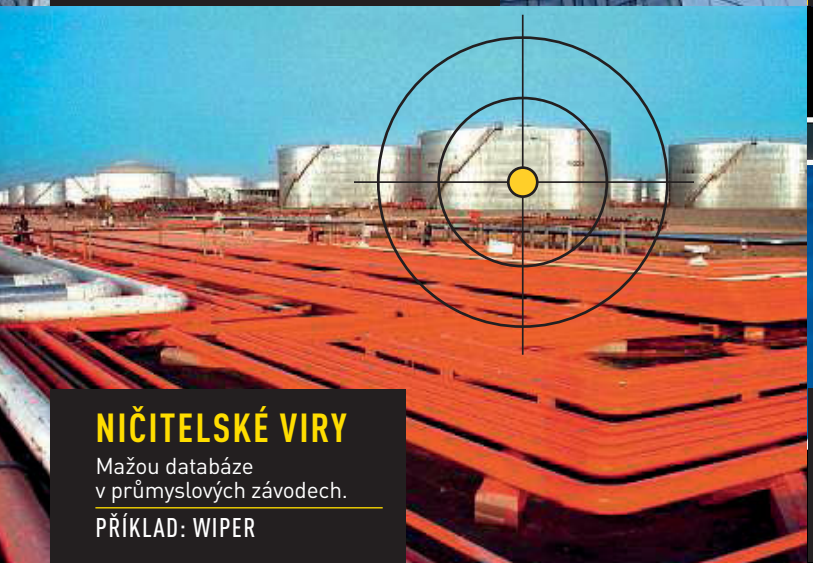
Kradou přístupové údaje a přesouvají peníze z účtu uživatele.

PŘÍKLAD: ZEUS CITADEL

MOBILNÍ VIRY

Shromažďují data uživatelů a odesílají drahé prémiové SMS.

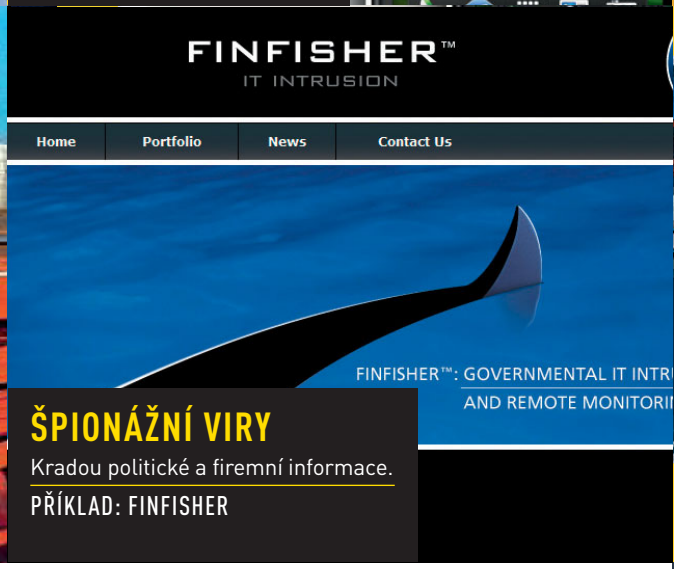
PŘÍKLAD: DROIDKUNGFU



NIČITELSKÉ VIRY

Mažou databáze v průmyslových závodech.

PŘÍKLAD: WIPER



ŠPIONÁŽNÍ VIRY

Kradou politické a firemní informace.

PŘÍKLAD: FINFISHER

SUPERVIRY budoucnosti

Pomocí nových triků krade malware peníze z účtů a špehuje uživatele – a to například i tehdy, když sedí před svým televizorem.

CLAUDIO MÜLLER, PETR KRATOCHVÍL

VLÁDNÍ TROJSKÉ KONĚ

Hledají v počítači citlivé informace.

PŘÍKLAD: BUNDESTROJAN

VIRY PRO SMART TV

Špehují uživatele pomocí kamer a mikrofonů.

PŘÍKLAD: LIGHTAIDRA

PRŮMYSLOVÉ VIRY

Manipulují s mechanickými výrobními stroji.

PŘÍKLAD: DUQU

EXPLOIT KITY

Infikují počítač malwarem přes softwarové zranitelnosti.

PŘÍKLAD: BLACKHOLE

FOTO: BUNDESKRIMINALAMT; GETTY IMAGES; ISTOCKPHOTO/GEORG WINKENS; REUTERS/STRINGER IRAN

Většina uživatelů pravděpodobně ví, že internet už dávno není bezpečné místo. Nepříjemnou realitou je ale fakt, že stále více z nich se o tom přesvědčuje na vlastní kůži – pro celou řadu lidí je šokující především skutečnost, že bezpečné už nemusí být ani na první pohled solidní stránky. Nedávno se o tom mohli přesvědčit například návštěvníci počítačového webu pcwelt.de v sousedním Německu. Útočníci totiž do kódu stránky propašovali 186 dílčích stránek, přes které se šířil do té doby neznámý malware, který z nakažených počítačů rozesílal spam. Ano, pro novou generaci robotů, špionážních nástrojů a bankovních trojských koní je typické, že k útoku byla zneužita na první pohled neškodná a zároveň důvěryhodná webová stránka.

Moderní malware sice nese na první pohled směšná a infantilní jména, jako Blackhole, GameOver nebo DroidKungFu, rozhodně to ale není hračka.

Aktuální superviry využívají bezpečnostní mezery v populárních softwarech (obvykle Java, Flash nebo Adobe Reader) a poté infikují miliony počítačů. Zajímavé jsou také cesty infekce. Stále větší oblibu získává metoda, při které zločinci umístí škodlivý kód na normální stránky nebo nalákají uživatele na stránky vlastnoručně připravené, v zapomnění ale neupadlo ani rozesílání upravených dokumentů. V tomto článku vám nejen prozradíme, proč je nový malware tak nebezpečný, ale zároveň vám i poradíme, jak se lze proti němu bránit.

Budoucí cíle: Windows 8 a Smart TV

Bezpečnostní experti očekávají, že v blízké budoucnosti se útoky zaměří také na Windows 8. Microsoft sice v novém operačním systému použil (ve srovnání s předchůdcem) větší množství bezpečnostních mechanismů, Arje Torersky, bezpečnostní specialista firmy Eset, ale tvrdí, že to nemusí stačit. Předpovídá, že hackeři budou využívat neznámé rozhraní k tomu, aby uživatele zmátli falešnými systémovými zprávami a donutili je zrušit bezpečnostní ochranu a umožnit malwaru cestu dovnitř.

Za zmínku také stojí, že jedna z nových bezpečnostních funkcí Windows 8 (ELAM – Early Launch Anti-Malware) již byla prolomena. „Už se objevily první rootkity, které se načtou ještě před jádrem OS, a tak obejdou ELAM," říká Stefan Wesche, bezpečnostní expert společnosti Symantec. Pravda ale je, že v současnosti dělají bezpečnostním expertům mnohem větší vrásky především smartphony, tablety nebo chytré TV. Ty totiž představují obrovské riziko, protože jejich obchody s aplikacemi jsou jen málokdy kontrolovány (Android), jejich uživatelé nemají téměř žádné bezpečnostní znalosti a návyky (Mac OS) nebo jsou na trh uváděna zařízení téměř bez bezpečnostního konceptu (Smart TV).

Experti odhadují, že soukromé hackerské skupiny budou využívat výše uvedené slabiny a své útoky budou stále více cílit na firmy, průmyslové podniky i politické instituce. Kvůli rostoucí aktivitě hackerů se také budou i k běžným zvědavcům dostávat nástroje na tvorbu malwaru a rootkitů. Například v Evropě se nedávno objevil na diskusních fórech špionážní software FinFisher, který byl až donedávna používán především na Východě a v Asii.

WINDOWS: Dojné krávy pro gangstery

Nové trojské koně zajišťují zločincům pohádkové zisky. Jejich triky: inteligentní botnety a seriózní IT podpora.

Pokud se počítačovému zločinci nedaří získat přístup do počítače oběti, zavolá „vrátnému“ a obdrží „univerzální klíč“. Jde o speciální software označovaný jako exploit kit, který obsahuje databázi známých i nových zranitelností. Díky nim se malware do počítače dostane pomocí Drive-by-Download, aniž by uživatel musel na cokoliv kliknout. Například při zmiňovaném útoku na IT magazín PCwelt prověřil exploit kit napadený počítač na čtyřicet mezer, než našel tu správnou a využil ji.

Podle našich informací patří v současné době k nejnebezpečnějším dostupným kitům nástroj Blackhole, který si lze (podle servisního dokumentu vývojářů) pronajmout už za 40 eur na den, roční verze stojí 1 200 eur. Zájemce pak jen začlení kód kitu na vybraný web a naláká na něj uživatele – například pomocí podvodných e-mailů. Ještě nebezpečnější je, když se zločincům podaří hacknout běžný web a do jeho struktury začlenit fragment kódu, který načte stránku s Blackholem neviditelně v pozadí. Exploit kit poté pomocí JavaScriptu prověří systém uživatele a detekuje jeho slabá místa. Zajímavé je, že všechny důležité informace získá malware z průběžně aktualizované databáze. Kit také analyzuje, který typ útoku bude nejvhodnější pro danou kombinaci Windows a příslušné verze dalšího nainstalovaného softwaru, a tyto informace ukládá pro pozdější použití. Od verze 2.0, která byla zveřejněna v září loňského roku, je tento malware pomocí bezpečnostního softwaru jen obtížně zjistitelný, a to i proto, že začal používat dynamické URL jak pro weby s Blackhole, tak i pro stránky, které hostí další malware.

O podnikavosti počítačových zločinců svědčí i skutečnost, že u kitu Blackhole existuje de luxe verze označovaná jako Cool Exploit Kit. Ta využívá pouze zero day zranitelnosti a díky tomu dokáže proniknout do libovolného počítače. Podle experta společnosti Symantec Stefana Wesche je tento nástroj vybraným zákazníkům k dispozici cca za 100 000 dolarů na rok.

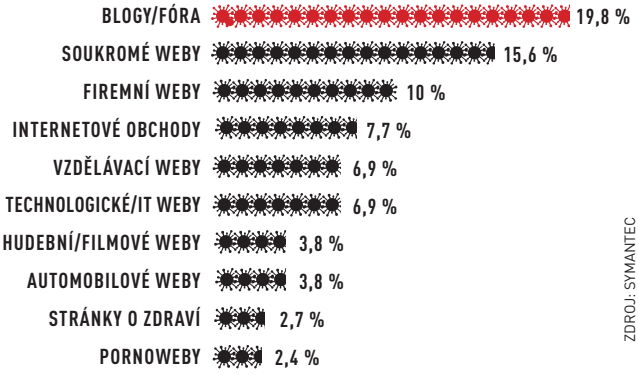
Klíč k 850 milionům počítačů

Jedním z největších úspěchů vývojářů kitu Blackhole byla zero day mezera v Javě, která byla objevena v lednu. Trvalo pět dní, než se vývojářům Javy ve firmě Oracle podařilo připravit záplatu. Během této doby útočníci převzali kontrolu nad obrovským množstvím počítačů a přesměrovali je na stránky infikované malwarem.

Mezi počítačovými zločinci je Java nesmírně oblíbená, protože je celosvětově instalována asi na 850 milionech počítačů a vzhledem k mizernému aktualizačnímu mechanismu je velké procento verzí beznadějně zastaralé.

JAK SE ŠÍŘÍ MALWARE

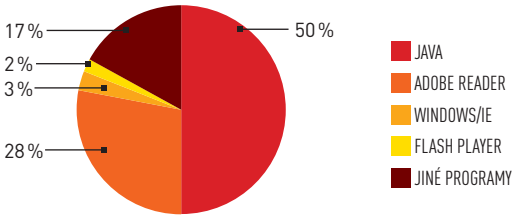
Zločinci se snaží hledat bezpečnostní mezery pro šíření malwaru u soukromých webů, které často používají nebezpečný (zranitelný) serverový software.



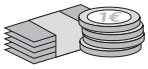
ZDROJ: SYMANTEC

VSTUPNÍ BRÁNY PRO MALWARE

Malware při průnicích do Windows využívá především bezpečnostní mezery v populárních programech.



ZDROJ: KASPERSKY



KOLIK STOJÍ VAŠE DATA

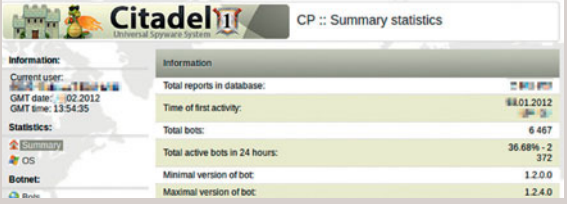
Chcete vědět, kolik za vaše data platí hackerům zlodějské podsvětí?

	HODNOTA
DATA O KREDITNÍCH KARTÁCH	112 €
E-MAILY, SMS	44 €
HISTORIE SURFOVÁNÍ	43 €
GPS-ÚDAJE	41 €
IDENTIFIKACE BROWSERU	39 €
PROFIL (ZÁLIBY, OBLÍBENÉ)	3 €
E-MAILOVÉ ADRESY, TELEFONNÍ ČÍSLA	3 €

ZDROJ: MCAFEE

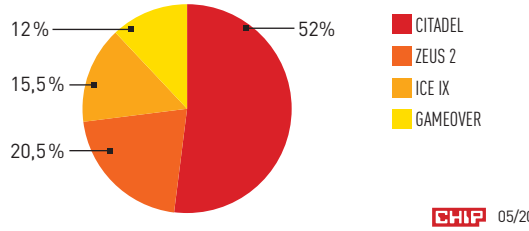
PROFESIONÁLNÍ BANKOVNÍ ZLODĚJI

Bankovní trojský kůň Citadel nabízí nejen panel pro ovládání botnetu, ale také fungující IT podporu.



ZEUS A JEHO ODNOŽE

Protože byl zdrojový kód malwaru Zeus zveřejněn na internetu, brzy se objevily nové a nebezpečnější verze tohoto bankovního trojského koně.



ZDROJ: F-SECURE

Pokud se exploit kitu podaří otevřít dveře do počítače, nejčastěji instalovaným malwarem jsou trojské koně. „Podle našich údajů je nejčastěji šířen především Citadel, klon trojského koně Zeus," říká Ralf Benzmüller, šéf bezpečnostní firmy G SecurityLabs. Pro tohoto trojského koně, označovaného jako číslo jedna, jeho vývojáři dokonce vytvořili on-line centrum péče o zákazníky, ve kterém si počítačoví zločinci mohou zažádat o nové funkce. Ty jsou poté vývojáři zapracovány do malwaru a objeví se v jeho nové verzi. Základní balíček Citadel obsahuje nástroj, kterým je možné vytvořit a řídit spam-botnet. Bezpečnostní expert Brain Krebs zjistil, že takovýto nástroj stojí jednorázově 2 400 dolarů plus měsíční poplatek 125 dolarů. Balíček ale může obsahovat i další moduly – například doplněk, který pomocí pravidelných aktualizací zajistí, že nástroj nebude detekován antivirovými nástroji. Tato funkce přijde na 395 dolarů za modul a 15 dolarů za aktualizace.

Budoucnost: Autonomní sítě botů

Budoucnost bankovních botnetů ukazuje GameOver, další varianta trojského koně Zeus. Ten není založen na klasické, centrálně řízené síti botů, ale jeho struktura ovládání spíše připomíná P2P sítě. V ní každý bot působí zároveň jako řídicí server a díky spojením s ostatními boty může být pravidelně informován o aktualizacích a tuto informaci může předat dále. Pro bezpečnostní složky je vypnutí takovéhoto botnetu velmi obtížné, protože nemá centrální řídicí bod, který by bylo možné odpojit od internetu. Stejně jako většina variant trojského koně Zeus také GameOver zaznamenává stisky klávesnice za účelem získání přihlašovacích údajů pro bankovní portály. Čas od času ale GameOver využívá také falešné bankovní weby, aby získal záznamy přímo. Odborníci očekávají, že P2P struktury sítě botů se budou dále rozvíjet a že na tento způsob řízení a výměny informací brzy přejdou všechny schopné malwary. Druhý dlouhodobě úspěšný způsob vydělávání peněz (kromě bankovních trojských koní) představuje ransomware – software vydírající uživatele.

Tento malware je založen na chytrém triku využívajícím psychologii. Uživatel obdrží zprávu o tom, že prováděl nelegální činnost (od návštěvy nezákonných webů přes stahování pirátských dat až po podporu terorismu), a proto je jeho počítač zablokován. Jeho činnost bude obnovena až po zaplacení pokuty. Obvyklou hrozbou je i to, že pokud uživatel nezaplatí do 24 hodin, budou z počítače vymazána všechna data. Seriózност tvrzení má podpořit celá řada log a certifikátů, obvykle od lokálních bezpečnostních firem a institucí. Zloději spoléhají na to, že naprostá většina uživatelů nějaký ten drobný hříšek na svědomí má, a pokud tento podvod neznají, obvykle zaplatí. Obvyklou „pokutou" je 50 až 100 eur; tato částka pak prostřednictvím anonymních platebních metod Ukash nebo Paysafe putuje na účty zločinců.

Z technologického hlediska existují dvě varianty tohoto softwaru: Reveton zcela blokuje přístup na plochu, Ransomcrypt zase šifruje jednotlivé dokumenty, nebo dokonce všechna data. Po zablokování přístupu má uživatel obvykle pět pokusů na zadání správného hesla. Pokud není heslo správné, trojský kůň se sám odstraní a nechá data zašifrovaná nebo systém zablokovaný.

Uživatelé by ale měli vědět, že platit někomu výpalné je zcela zbytečné. Naprostá většina elitních bezpečnostních firem na svých webech nabízí programy, kterými lze takto postižené systémy odemknout a vyčistit. Například na webu firmy Kaspersky najdete nástroj Unlocker, který dokáže odblokovat plochu, a například u Aviry najdete Ransom File Unlocker, který dešifruje a obnoví počítače napadené malwarem Ransomcrypt.

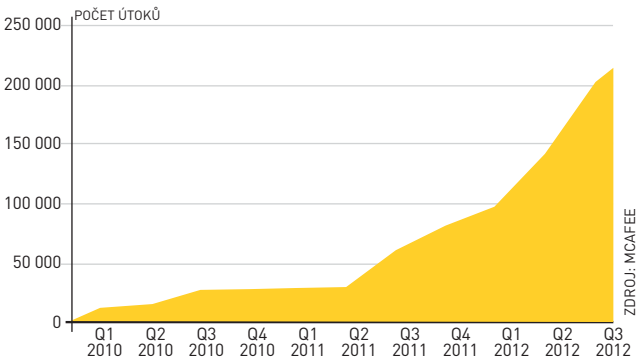
ZAPLAŤTE, NEBO PŘIJDETE O DATA!

Oblíbené jsou také vyděračské malwary, které vám zašifrují počítač. K datům pak dostanete přístup až poté, co zaplatíte. Postupem času přišli zloději na to, že ještě lepší je zaštítit se oficiálními autoritami – například policií. Uživatelé s pocitem viny pak ochotněji zaplatí. První verze tohoto malwaru používala špatnou češtinu, takže zaplatili skutečně jen extrémně naivní uživatelé.

Druhá verze už disponovala mnohem důvěryhodnějším vzhledem a také použitému jazyku už téměř nebylo co vytknout.

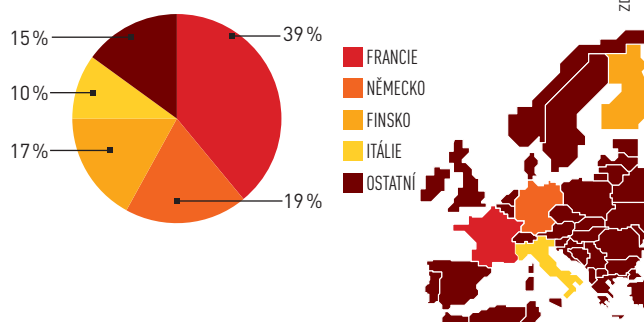
ÚSPĚŠNÍ VYDĚRAČI

V loňském roce také rapidně vzrostl počet obětí počítačových vyděračů.



KDE TAKÉ VYDÍRAJÍ?

Podobné vyděračské malwary fungují i v dalších zemích – jsou lokalizované a podobně úspěšné.



MOBILY & TV:
Hřiště pro hackery

Sotva se zločinci zabydleli v OS Android, už se připravují na útok na další zařízení. Tentokrát mají na mušce chytré televizory.

První viry pro mobilní zařízení byly na první pohled neškodné – často útočily jen na několik zařízení a i škody jimi způsobené byly spíše symbolické. Šlo však jen o prototypy a po zahřívacím kole přichází jejich nástupci, kteří už představují skutečnou hrozbu. Například v polovině ledna objevila bezpečnostní firma Kingsoft botnet s více než milionem ovládnutých smartphonů. V 7 000 aplikacích v alternativních obchodech s aplikacemi byl také nalezen špionážní trojský kůň. Vývojáři mobilního malwaru si již otestovali své schopnosti a nyní přechází do protiútoku.

Podobný vývoj probíhá i na platformě Mac. Zatímco první pokusy byly neškodné, v minulém roce už podle firmy F-Secure dokázali hackeři infikovat 600 tisíc Maců spamovým trojským koněm. Pro velký úspěch by chtěli počítačoví zločinci podobný útok zopakovat i na dalších zařízeních, která lze připojit k internetu: na televizorech, DVD přehrávačích a set-top boxech.

Pokud jsou tato zařízení integrována v domácí síti, mohou útočníci infiltrovat malware na PC a odtud proniknout do těchto koncových zařízení. Pro škůdce totiž obvykle není problém proniknout přes otevřené síťové porty, které ve většině případů nejsou chráněny, v nejlepším případě pouze jednoduchým heslem. Jeden z prvních útoků na zařízení schopná pracovat s internetem proběhl už na konci loňského roku, kdy malware LightAidra infikoval set-top boxy, IPTV zařízení a routery, které využívaly linuxové systémy MIPS nebo SuperH.

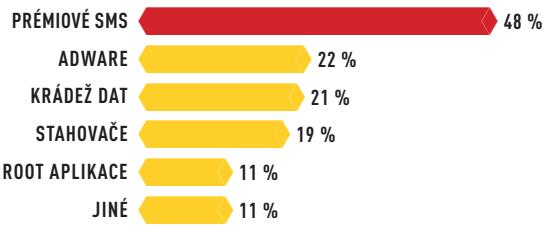
Hackeři, kteří se dívají do obývacího pokoje

Jaké škody může takovýto malware nadělat, to nám bezpečnostní expert předvedl na televizorech Samsung a Sony Bravia. Oba dva přístroje mohly být z počítače zmanipulovány takovým způsobem, že se z nich stal jen bezcenný kus nábytku: po úpravě se televizory neustále restartovaly. V TV Samsung proběhl útok pomocí zmanipulovaných datových paketů putujících do síťového portu zařízení. V televizoru Sony-Bravia nahradil útočník MAC-adresu televize dlouhým řetězcem znaků, který vytvořil přetečení vyrovnávací paměti v paměti přístroje. Podle bezpečnostního experta Gabriela Menezese lze v tomto řetězci znaků skrýt malware a poté ho spustit v přístroji. V prosinci loňského roku navíc objevila bezpečnostní firma ReVuln v Samsung Smart TV další mezeru, která umožňuje útočníkům zjistit sledované kanály a také číst data z připojených USB datových nosičů.

Ještě děsivější však může být představa opravdových televizních virů. Je nutné si uvědomit, že celá řada nejnovějších televizorů má integrovanou kameru a mikrofon, které se odpojují pouze softwarově, a nikoliv fyzicky. Pokud je bezpečnostní ochrana zařízení nedostatečná, mohou být útočníci schopni mikrofony a kamery aktivovat a pak vás v obývacím pokoji sledovat. Novější modely televizorů navíc obsahují výkonné procesory, které lze snadno zneužít k nelegálním aktivitám.

NEJČASTĚJŠÍ CÍLE ÚTOKŮ NA ANDROID

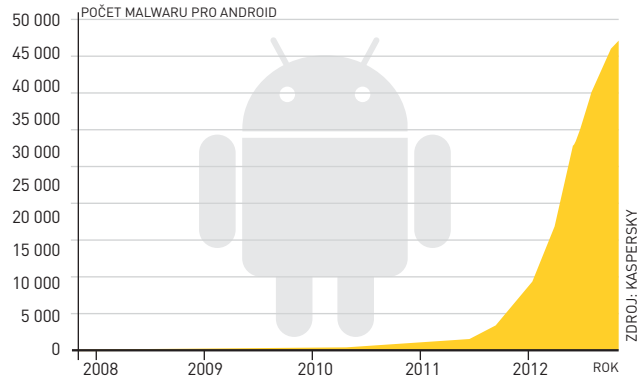
Většina malwaru pro Android cílí na více oblastí, takže součet hodnot v grafu přesahuje 100 procent.



ZDROJ: TREND MICRO

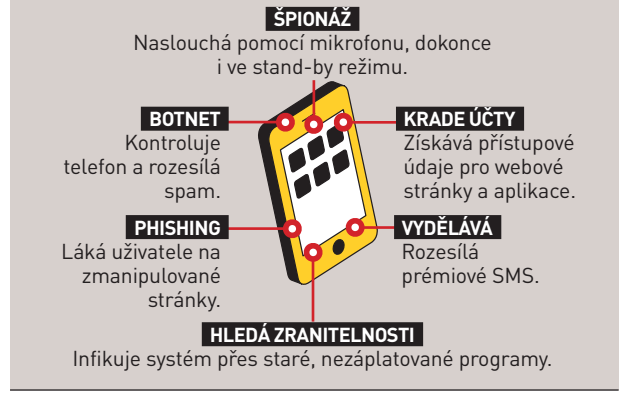
MALWARE PRO ANDROID SÍLÍ

Zvyšující se počet malwaru pro mobilní zařízení není překvapující. Rychlost, jakou vznikají nové varianty, je ale děsivá.



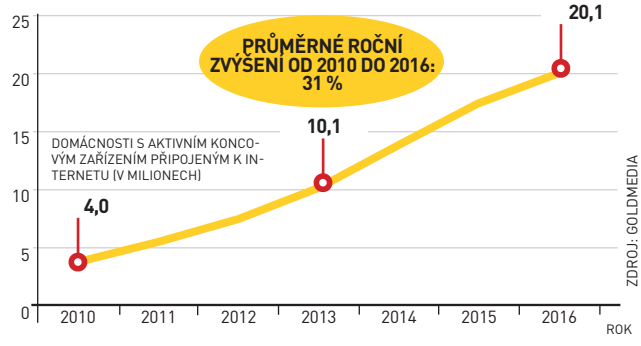
ZDROJ: KASPERSKY

CO UMÍ MALWARE VE SMARTPHONU



VÝVOJ POČTU SMART TV

Data ze sousedního Německa naznačují velký potenciál chytrých televizorů, schopných pracovat s internetem, jako cílů pro hackery.



ZDROJ: GOLDMEDIA

PLACENÁ INZERCE

PRŮMYSL: Digitální válka

Komplexní, profesionálně vyvinutý malware útočí na ekonomiku a politické subjekty. Profesionální špionážní software navíc může zůstat neodhalen celé roky.

Nejnebezpečnější viry nenapadají počítače, ale elektrické sítě, útočí na bankovní pobočky nebo špehují politické orgány. Útočníci, soukromé hackerské skupiny, nebo dokonce tajné služby tyto operace plánují pečlivě – například špionážní akci známou pod jménem Red October objevila až letos v lednu firma Kaspersky. V rámci této akce byly z diplomatických úřadů, výzkumných ústavů a vládních organizací celosvětově shromažďovány geopolitické informace. Cílené útoky začaly phishingovými e-maily, nabízejícími koupi diplomatických vozidel, a vedly k nainstalování malwaru využívajícího zranitelností Wordu a Excelu.

„Ačkoliv to rozhodně nebyl originální útok, špionáž úspěšně fungovala více než pět let," říká Magnus Kalkuhl, šéf bezpečnostního teamu Kaspersky. Přibližně třicet modulů v malwaru použitém k útoku dokázalo číst hesla, kopírovat e-maily z poštovních serverů, získávat záznamy klávesnice nebo infikovat mobilní telefony a USB zařízení připojená k počítači. Malware navíc obsahoval i kryptografický modul, který dokázal číst dokumenty zašifrované pomocí nástroje Acid Cryptofiles, pomocí něhož NATO, Evropský parlament a Evropská komise chrání svá tajná data.

„Kromě toho obsahoval Red October také rafinovanou samoobnovovací rutinu, která umožňovala při nové infekci prostřednictvím e-mailu znovu malware rychle aktivovat, i pokud byly jeho hlavní komponenty ze systému odstraněny," říká Kalkuhl. Podle názoru expertů je pravděpodobné, že útok probíhal z rusky mluvící oblasti, nicméně exploit využívající zranitelnosti v kancelářském softwaru pocházel od čínských hackerů. Za zmínku také stojí, že pět dní poté, co se této operaci dostalo pozornosti světového tisku, byly vypnuty všechny servery používané v akci.

Protiútoky na západní banky

Nedávno byla celá česká IT republika na nohou a se zděšením sledovala DDoS útoky na významné domácí cíle, v západní Evropě již byly podobné útoky zaznamenány v loňském roce.

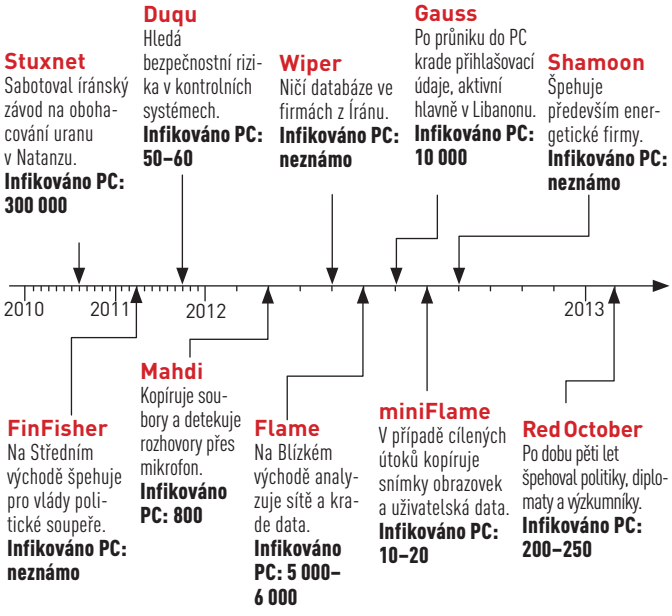
Podle bezpečnostních expertů špehovaly americké tajné služby na Středním východě pomocí malwaru Flame a v září, krátce po odhalení, se dostaly pod palbu irácких hackerských skupin americké banky. Podle dostupných informací stála za útoky íránská organizace kyberbojovníků Qassam, kterou prý najala íránská vláda. Té se podařilo pomocí DDoS útoků ochromit platební služby bank a vyřadit z provozu jejich servery. Útoky se opakovaly a na počátku tohoto roku dosáhly takové intenzity, že banky požádaly o pomoc americké tajné služby.

Ačkoliv pro většinu uživatelů jsou podobné útoky jen titulkem v novinách, je nutné si uvědomit, že půjde-li dnes o krátký útok na banky či zpravodajské weby, zítra mohou být napadeny energetické rozvody či elektrárny.

AUTOR@CHIP.CZ

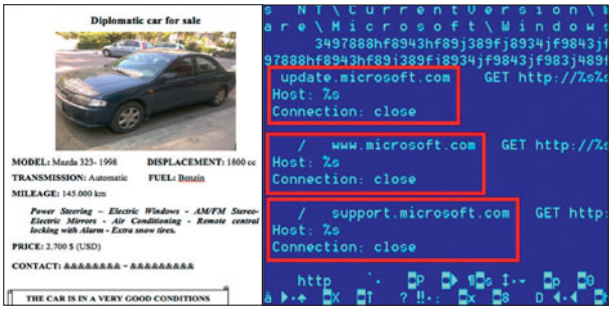
KYBERNETICKÉ ÚTOKY POSLEDNÍCH LET

Není jasné, zda počet kybernetických útoků roste, nebo zda jich detekujeme více. V každém případě se ale zvyšuje složitost útoků.



JAK RED OCTOBER OVLIVNÍ POČÍTAČE

Pomocí infikovaných phishingových e-mailů je do počítače propašován malware, který ihned po instalaci zablokuje aktualizace Windows.



RED OCTOBER ŠPEHUJE

Poté, co malware nahraje různé moduly, jako například keylogger, začne posílat data do řídicího serveru.