Router Turris (foto CZ.NIC)

Projekt Turris v roce 2014

Bedřich Košata

Projekt Turris je výzkumnou aktivitou sdružení CZ.NIC, správce české národní domény .CZ, zaměřenou na bezpečnost v domácích sítích. Hlavním cílem projektu je s pomocí specializovaného routeru sledovat síťový provoz mezi domácí sítí a Internetem a nabízet uživateli zvýšenou ochranu před útoky. Projekt byl veřejnosti představen v polovině roku 2013 a v tomto článku si zrekapitulujeme jeho vývoj v roce 2014 a nahlédneme do plánů jeho dalšího možného směrování.

Router Turris

Vzhledem ke specifickým požadavkům na výkon a vlastnosti routeru pro bezpečnostní analýzu jsme po průzkumu běžně dostupných zařízení dospěli k myšlence vývoje vlastního řešení. Tak vznikl v Laboratořích CZ.NIC vlastní hardwarový návrh, který byl později pojmenován router Turris. Ten je založen na výkonném dvoujádrovém procesoru platformy PowerPC, který zvládá implementované bezpečnostní analýzy bez zpomalení sítě i při rychlostech v řádu stovek megabitů za sekundu.

Sériová výroba 1000 kusů routeru Turris byla po třech prototypových sériích zahájena na konci roku 2013 a probíhala i na začátku roku 2014, kdy jsme pro zařízení získali certifikace pro použití v EU. To byla poslední překážka pro distribuci uživatelům, kterou jsme následně zahájili a probíhala až do konce prázdnin.

Vzhledem k tomu, že se ukázalo, že zájem o účast v projektu je výrazně vyšší, než jsme původně očekávali, rozhodli jsme pro výrobu další tisícové série. V tomto případě jsme chtěli využít zkušenosti z provozu první verze a ohlasy uživatelů a mírně zařízení vylepšit. Vznikl tak router Turris verze 1.1, který je v době vzniku tohoto článku ve výrobě a bude dostupný uživatelům na přelomu roku.

Kromě interních změn, jako je optimalizace zdrojů napájení, došlo k několika vylepšením viditelným pro uživatele. Na první pohled si uživatelé jistě všimnou zejména třetího USB portu, který je umístěn na předním čele routeru a na rozdíl od zadních portů, které využívají standard USB 2.0, se jedná o novou verzi USB 3.0. To určitě potěší každého, kdo chce mít doma superrychlý NAS postavený z routeru. Další novinkou je vylepšená podpora pro miniPCIe karty, zejména s ohledem na záložní mobilní připojení. Byla výrazně vylepšena jejich podpora a na desku routeru přibyl slot pro SIM kartu, který je s miniPCIe konektorem propojený a umožňuje tak použít i karty, které vlastní slot nemají (typicky používané v noteboocích).

Na první pohled viditelnou změnou je také vzhled routeru, který již na vrchním krytu nemá charakteristickou perforaci ve tvaru loga .cz, ale je plný. Důvodem je změna chlazení procesoru routeru pomocí teplovodivého propojení procesoru s kovovým krytem routeru, což umožnilo snížit jeho teplotu o 10–20 °C v závislosti na jeho zatížení.

DSL modem Turris

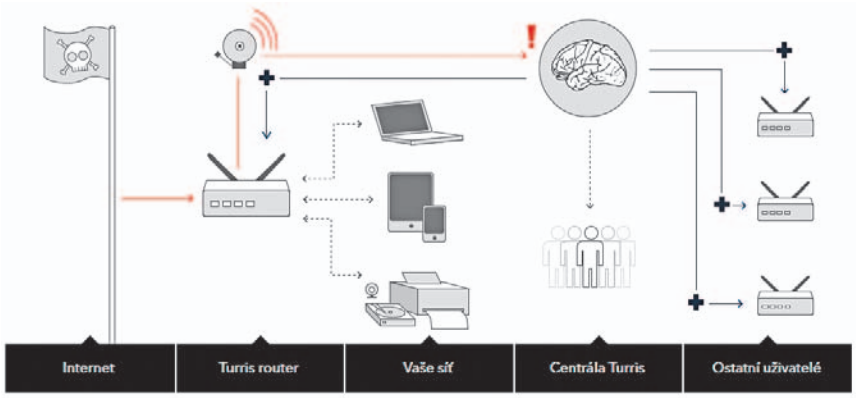
Cílem projektu Turris bylo od počátku dosáhnout co nejrovnoměrnější distribuce routerů po České republice, ať již z pohledu jednotlivých poskytovatelů připojení (ISP) nebo geografického. Toho se díky postupné distribuci routerů a výběru uchazečů podařilo velmi dobře dosáhnout. Jedinou výjimkou byly sítě, které využívají telefonní kabeláž, tedy DSL připojení. Takoví uživatelé mají již

často modem ve formě plnohodnotného routeru od poskytovatele a vzhledem k tomu, že router Turris nemá DSL rozhraní, musí provozovat obě tato zařízení současně, což je nevýhodné. Z tohoto důvodu jsme se rozhodli zároveň s novou sérií routerů vyvinout i malý, jednoduchý a energeticky úsporný DSL modem, který by byl přímo šitý na míru routeru Turris a eliminoval nutnost použití běžného DSL modemu.

Stejně jako v případě routeru Turris jsme se pokoušeli takové zařízení najít na trhu, ale to se nám bohužel nepodařilo. To byl hlavní impulz pro vývoj vlastního řešení. Výsledkem vývoje je zařízení o rozměrech balíčku karet, které je schopné router Turris připojit k síti s pomocí technologií ADSL i VDSL ve všech rychlostech nabízených na českém trhu. Toto zařízení bude podobně jako router Turris 1.1 k dispozici na přelomu roku 2014 a 2015.

Turris OS

Spolu s vlastním hardware vyvíjí CZ.NIC pro své routery i vlastní programové vybavení včetně operačního systému. Ten samozřejmě nevzniká na zelené louce, ale jako dlouhodobí uživatelé a producenti otevřeného software stavíme na existujícím řešení, kterým



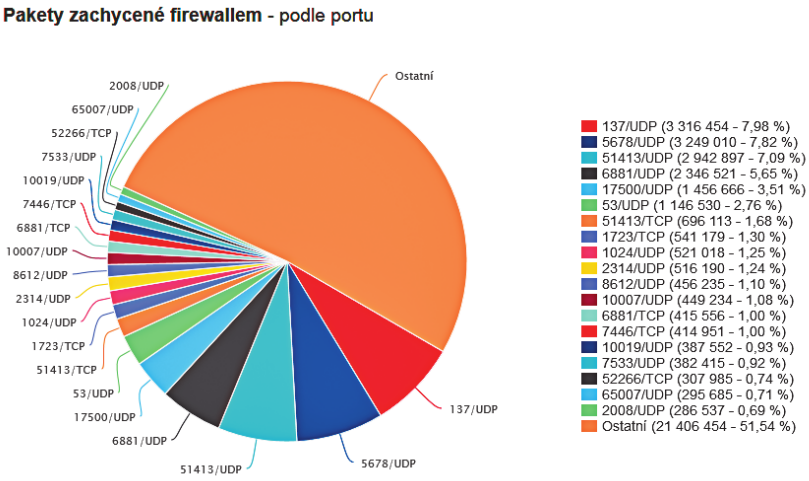
je Linuxová distribuce OpenWrt optimalizovaná pro domácí routery.

Operační systém routeru, který nazýváme Turris OS, upravuje OpenWrt tak, že přidává některé funkce, jako je podpora DNSSEC, a snaží se držet více konzervativní přístup k aktualizacím systému. To ale rozhodně neznamená, že bychom systém nerozvíjeli. Naopak, díky systému automatických aktualizací můžeme velice rychle reagovat na případné nové hrozby a také router vylepšovat bez nutnosti zásahu uživatele. V roce 2014 jsme vydali 8 větších aktualizací systému a několik rychlých oprav, mezi kterými stojí za zmínku jistě oprava chyby OpenSSL Heartbleed nebo aktualizace programu Bash po odhalení chyby Shellshock. V obou případech byly bezpečné verze děravých programů na routerech všech uživatelů k dispozici v řádu dní od jejich zveřejnění.

Bezpečnostní výzkum

Kromě vývoje v oblasti hardware a operačního systému jsme se samozřejmě intenzivně věnovali i hlavnímu poslání projektu a to je bezpečnostní výzkum v oblasti síťových útoků a domácích sítí.

Výrazně jsme rozšířili množství sond, které na routeru Turris běží a sledují procházející provoz. Kromě jednoduché sondy, která slouží ke sběru obecných informacích o datovém provozu, jako je množství přenesených dat,



Statistiky – pakety podle portu

využití jednotlivých protokolů, atp., obsahuje router sondy na statistickou detekci síťových anomálií, monitorování spojení s podezřelými adresami nebo detekci velkého množství nenavázaných spojení z vnitřní sítě. Dále jsou obsaženy také aktivní sondy, které testují, zda router dostává správné odpovědi na DNS dotazy, nebo zda routery umístěné v různých sítích dostávají stejné certifikáty od důležitých serverů (jako jsou servery bank, e-mailových služeb, sociálních sítí) a nedochází tedy k lokálním útokům typu man-in-the-middle.

Důležitým zdrojem informací o útocích jsou také záznamy firewallu jednotlivých zařízení, které jsou centrálně analyzovány a mimo jiné na jejich základě publikujeme tzv. „greylist“, tedy seznam adres, které se chovají podezřele, protože se snaží připojovat na větší množství routerů na důležité služby, jako je SSH či Samba. Tento seznam používáme také jako jeden ze zdrojů dat pro sběr informací o spojeních s podezřelými adresami a již jsme s jeho pomocí pomohli několika uživatelům detekovat nebezpečné nastavení jejich sítě. Podobně využíváme také veřejně dostupné zdroje informací o velících centrech botnetů a v případě zjištění komunikace klienta s takovou adresou jej informujeme.

Celé toto portfolio sond nám umožňuje v případě různých bezpečnostních anomálií nebo incidentů posoudit situaci z různých úhlů pohledu. Za rok 2014 se nám tak podařilo již u šestnácti uživatelů prokazatelně odhalit nákazu nějakým druhem malware, přičemž u další podobně velké skupiny uživatelů nemáme tuto skutečnost plně potvrzenou.

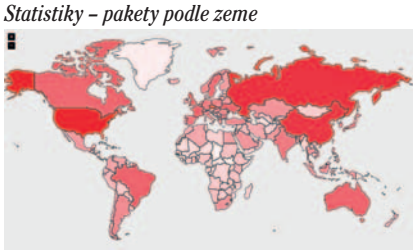
Kromě detekce malware u jednotlivých uživatelů se snažíme ale také o ucelenější analýzy síťového provozu, které by mohly směřovat k odhalování větších hrozeb, např. organizovaného postupu více strojů zapojených v botnetu. Na tyto analýzy používáme několik metod, které posuzují podobnost chování různých adres zachycených na firewallu routerů nebo v našich honey-potech a snaží se odhalovat podobně se projevující stroje. U nich je pak velká pravděpodobnost, že jsou ovládány z jednoho zdroje a mohou být tedy zapojeny do botnetu. Tato část analýzy je v okamžiku vzniku tohoto článku ve stádiu ladění, ale již nyní máme vytipováno několik skupin počítačů, u nichž sledujeme dlouhodobější vývoj, abychom posoudili jejich skutečnou součinnost a nebezpečnost.

Sběr statistických údajů

Na webových stránkách projektu Turris (www.turris.cz) dáváme uživatelům k dispozici statistický přehled o datech, která jsme u nich nasbírali, a některá z nich využíváme také v globálních statistikách, které jsou dostupné veřejnosti.

K dispozici je např. statistika zastoupení protokolu IPv6 v celkovém provozu, informace o službách, které jsou nejčastějším cílem nevyžádaných pokusů o spojení, nebo mapa zemí, ze kterých taková spojení přicházejí. Nově jsme také v poslední době přidali výsledky pasivního monitoringu rychlosti připojení jednotlivých uživatelů. Tato metoda na rozdíl od běžného měření rychlosti nepoužívá vlastní vygenerovaný provoz, ale využívá provoz, který již na routeru přirozeně je. Má tedy výhodu, že může běžet 24 hodin denně bez vlivu na množství přenesených dat (nevýhodou samozřejmě je, že linka musí být plně využita, aby byla metoda účinná - proto zaznamenáváme v daném časovém úseku maximální dosaženou rychlost). Výsledky této statistiky jsou k dispozici také v sumarizované podobě ve veřejných statistikách projektu. Vychází z nich například, že polovina uživatelů má rychlost připojení vyšší než 20 Mbit/s. Nově tuto statistiku rozšíříme o informace, kolik času je linka využitá do jaké míry, což by mohlo uživatelům napovědět, jak linku využívají a zda je pro ně dostatečná.

Statistiky – pakety podle zeme



Kromě informací, které hromadně sbíráme a vyhodnocujeme, nabízíme uživatelům také čistě privátní informace. Zde je nejzajímavější aplikace Majordomo, která umožňuje majiteli routeru udělat si přehled o tom, jak jeho domácí zařízení komunikují s Internetem. Tato funkce byla implementována jako reakce na kauzu chytrých televizí, které vynášely informace o domácí síti k výrobci, ale lze ji použít i k dalším účelům, např. k rozdělení nákladů při sdílení připojení.

Budoucnost projektu Turris

Po umístění dalšího tisíce routerů Turris v českých sítích již nevidíme velký přínos v rozšiřování jejich množství. Budeme se tedy zaměřovat zejména na jejich maximální využití pro účely výzkumu a dále budeme samozřejmě vylepšovat systém routeru.

Zajímavým výsledkem představování routeru Turris v zahraničí byla zejména poptávka po otevřeném hardware, který plně podporuje OpenWrt a také ohlas na automatické aktualizace routeru, což je oblast, která je mnoha odborníky považována za hlavní slabinu dnešních domácích routerů.

Na základě tohoto ohlasu zvažujeme zaměřit v roce 2015 vývoj hardware na dostupný otevřený domácí router, který by byl k dispozici komerčně. Jeho hlavními devizami by měla být kromě otevřenosti i velká rozšiřitelnost a bezpečnost vestavěná do systému. V této oblasti bychom využili zkušeností s vývojem a údržbou bezpečného operačního systému a nabídli bychom uživatelům také náš Turris OS. Tento produkt je zatím ve stádiu příprav pod kódovým názvem Turris Lite. Zájemci o jeho vývoj se mohou zaregistrovat na stránkách lite.turris.cz. ■

Autor článku, Bedřich Košata, je vedoucím vývojového týmu projektu Turris (sdružení CZ.NIC)