Projekt Turris **chrání i vás**

Jaké jsou cíle projektu Turris a daří se je plnit? Co si tvůrci slibují od druhé generace? Na to jsme se zeptali Ondřeje Filipa, výkonného ředitele společnosti CZ.NIC. [Jiří Kuruc]

V minulém čísle Computeru jsme přinesli pohled na druhou generaci ryze českého routeru Turris Omnia, který vznikne mimo jiné i díky úspěšné kampani na Indiegogo. Projekt Turris však není jen o super výkonném routeru, týká se především bezpečnosti, jak nám upřesnil Ondřej Filip.

Projekt Turris vznikl již před dvěma lety, mezi veřejností se však stále drží spousta polopravd a omylů. Co je projekt Turris a jaké jsou jeho hlavní cíle?
Projekt Turris si již od začátku stanovil více cílů: Prvním cílem bylo vyvinout bezpečný firmware pro domácí routery. Tedy takový, který by se automaticky aktualizoval, který by laickému uživateli nedovolil nebezpečnou konfiguraci a který by reagoval na aktuální bezpečnostní situaci. Druhým cílem bylo ukázat, že domácí router může plnit i další úkoly pro uživatele než jen routing. Uvědomme si, že ve většině domácností je právě router jediné zařízení, které má procesor a které je zapnuté non-stop. A třetím a možná nejviditelnějším cílem bylo vybudovat síť sond, které budou sbírat informace o bezpečnostních problémech u domácích uživatelů. Součástí tohoto třetího cíle byla analýza informací a následná publikace útočících IP adres či pravidel do firewallu/IPS.

Co všechno jste díky routerům schopni odhalit?
Turris je v první řadě schopen odhalit napadená a někdy i špatně nakonfigurovaná zařízení v síti uživatele, díky tomu, jak detekuje podezřelé toky z domácí sítě ven do Internetu. Dále posílá informace o útocích, které odrazil, a také funguje jako tzv. honeypot neboli tváří se sám jako napadnutelné zařízení a poté analyzuje chování útočníka, který se mylně domnívá, že se mu zdařil útok. Díky tomuto jsme schopni sledovat aktivity některých botnetů, zdroje a četnosti útoků na konkrétní služby apod.

Podařilo se cíle v uplynulých dvou letech naplnit? Zjistili jste konkrétní bezpečnostní problémy?
Řekl bych, že stanovené cíle se naplnit podařilo. V bezpečnostní oblasti jsme vyvinuli nové metody, jak sledovat aktivitu botnetů, publikujeme zmiňovaný seznam podezřelých IP adres, detekujeme tisíce útoků denně. Podařilo se nám detekovat malware v domácích sítích uživatelů Turrisů a analyzovali jsme chování několika větších botnetů. Nejzajímavější je například botnet, který obsahuje přes 32 tisíc domácích routerů Asus. Zde tkví problém především v tom, že administrace routeru při vyhledání nového firmwaru oznámí, že používá nejnovější verzi, ačkoli to není pravda a na stránkách výrobce již lze stáhnout nové verze, které mají kritické chyby opraveny.

„Výrobci nejrůznějších zařízení nejsou příliš aktivní v opravách chyb“

V dalších zmíněných oblastech jsme také uspěli. Náš operační systém Turris OS se sám aktualizuje na dvou tisícovkách zařízení a mnoho uživatelů náš router využívá i k dalším funkcím. Kromě častého využití pro domácí úložiště sem patří třeba i streamování videa z digitálního vysílání, monitoring chytré domácnosti a podobně.

Jak výsledky těchto měření přetavíte v praktická opatření? Jste například ve spojení s výrobci špatně zabezpečených zařízení?
Snažíme se pochopitelně veškerá naše zjištění publikovat. Nicméně obecně je určitým zklamáním, že výrobci těchto zařízení nejsou příliš aktivní v opravách chyb. Často se chybný firmware objevuje i dlouho poté, co je popis chyby zveřejněn.

Samozřejmě ale nečekáme jen na reakce výrobců a v závažných případech s uživateli aktivně komunikujeme sami. Na tomto se podílí kolegové z našeho CSIRT týmu, kteří v případě detekce nákazy v síti pomáhají situaci řešit přímo s uživatelem. Už se nám tak na základě externího síťového provozu podařilo detekovat malware ve vnitřní síti několika desítek uživatelů a pomoci jim ho odstranit.

Druhá generace routeru Omnia se těší ohromnému celosvětovému zájmu. Přichází s druhou generací nové cíle a úkoly?
Zatímco první generace routerů Turris plnily především cíle v oblasti bezpečnosti, u druhé generace, tedy u řady Turris Omnia, půjde především o to, zdali se prosadí na trhu. Pevně věříme, že se zcela odlišuje od stávajících produktů v kategorii SOHO routerů. Její popularita bude pochopitelně záviset na tom, zdali jsme dobře zvládli první a druhý jmenovaný cíl projektu, tedy vývoj bezpečného firmwaru a další využitelnost routeru v domácnostech a firmách.

Doposud působil projekt především na českém trhu, generace druhá se však podívá do celého světa, navíc v mnohem větším množství. Jste na to připraveni?
Pevně věříme, že ano. Výroba a distribuce druhé generace bude pochopitelně výrazně náročnější. Uživatelé první generace byli téměř výhradně Češi. Druhou generaci, tedy Turris Omnia, si již objednali uživatelé skutečně z celého světa, ze všech osídlených kontinentů, což pochopitelně klade velké nároky na přípravu logistiky, na certifikace pro jednotlivé trhy, jazykové mutace a podobně. Stejně tak bude výrazně vyšší množství vyrobených kusů a to je poněkud náročnější i s ohledem na to, že výrobu chceme i nadále zachovat v České republice, což pochopitelně není v tomto oboru typická výrobní země. Nicméně pevně věříme, že jsme nic v tomto směru nepodcenili a v blízké budoucnosti výroba a distribuce nastartuje. ■