Zranitelné směrovače

Na uživatele domácích routerů směřuje více než 250 útoků denně.

JIŘÍ PRŮŠA

O tom, jak zranitelné mohou být SOHO routery, se lze prakticky každý týden dočíst v analýzách nejrůznějších bezpečnostních firem. Třeba zpráva společnosti Symantec uvádí meziroční nárůst počtu útoků na IoT zařízení o 600 %.

Mezi nejzranitelnější pak patří nezabezpečené routery, prostřednictvím kterých je často možné získat snadný přístup k jednotlivým připojeným zařízením. O narůstajícím počtu útoků na síťová zařízení a jejich závažnosti svědčí rovněž jarní varování oficiální americké organizace CERT.

Převést všechny tyto útoky a výsledky práce analytiků do srozumitelnějších čísel se pokusilo sdružení CZ.NIC v rámci projektu Honeypot as a Service (HaaS), který nabízí možnost přesměrování útočníků na centrální honeypot.

Co se zjistilo?

Do projektu podpořeného Technologickou agenturou ČR se podařilo zapojit již více než 2 000 uživatelů, z nichž necelé tři čtvrtiny tvoří uživatelé routerů Turris.

Vysoký počet uživatelů se následně odrazil rovněž na objemu zachycených dat, resp. sezení a příkazů, které útočníci na centrálním honeypotu uskutečnili.

Na cílovém honeypotu, na který byli útočníci přesměrováváni, bylo za první pololetí letošního roku celkem zaznamenáno více než 73 milionů sezení a téměř 42 milionů příkazů (někteří útočníci neuskutečnili žádný příkaz), viz příslušný graf.

Pokud se přistoupí na prostou kalkulaci, že jedno sezení se rovná jeden pokus dostat se do routeru, vychází, že každý den je „vstupní brána internetu“ cílem i více než 250 útoků, to znamená přibližně deseti útoků za hodinu.

Je sice pravda, že ne všechny pokusy představují sofistikované útoky, avšak podrobnější analýza ukazuje, že v některých případech by útočník mohl napáchat významné škody.

Nahlédnout útočníkům více pod prsty umožnila analýza jednotlivých vzorků, která byla v rámci projektu HaaS ukutečněna ve spolupráci s tchajwanským partnerem – Institute for Information Industry (III).

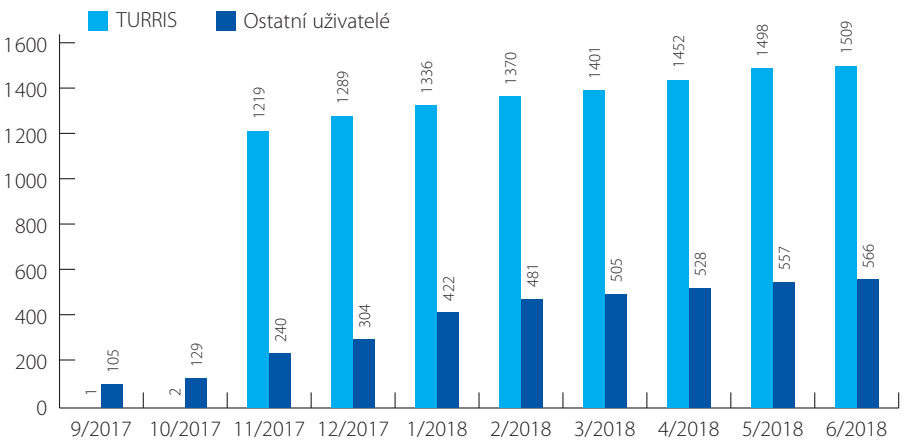
Za první pololetí letošního roku se na server nahrálo celkem 8 071 unikátních souborů zabírající v součtu více než 6 GB. Díky tomu, že se zkoumaly pouze unikátní soubory (tj. pokud byl soubor zachycen v únoru, jeho další zachycení v březnu se již nezapočítává), je klesající tendence zachycených vzorků logická.

Co se týče cílových architektur, zachycené binární soubory byly velmi rozmanité – od ARM přes MIPS až po x86 včetně nejrůznějších podvariant. Dva největší soubory měly stejný začátek jako instalační media Debian 9.3 a Linux Mint 18.3, což se dá nejpravděpodobněji vysvětlit snahou útočníků ověřit, kolik si můžou na nově získaný stroj uložit dat.

Dalším zajímavým nálezem byl 17MB textový soubor obsahující přes milion domén, ze kterých se 945 nacházelo v doméně .CZ. Vzhledem k faktu, že se mezi českými doménami nápadně často vyskytovaly domény státní správy, byl tento soubor poskytnutý Národnímu úřadu pro kybernetickou bezpečnost (NÚKIB).

Na základě provedené dynamické analýzy byly odhalené například snahy o komunikaci s Command and Control (C&C) serverem, to jest řídicím počítačem pro sítě botnet.

Počty uživatelů HaaS



Počty zachycených sezení a příkazů