Atak na české routery

Když v prvním týdnu letošního května Národní bezpečnostní tým Csirt.cz přijal informaci o napadeném routeru TP-Link, který počítače a další připojená řešení pomocí změněného DNS serveru přesměrovával na podvržené stránky, tamní experti tušili, že jde o závažný problém. Překvapení jim ale přinesl počet zařízení, která jsou v Česku tímto útokem ohrožena.

PAVEL BAŠTA

Problém označovaný jako SoHo Pharming spočívá v tom, že někdo napadá několik vybraných značek routerů, převážně z produkce firmy TP-Link, ale i další, a na těchto zařízeních mění primární DNS server.

Ten pak uživatelům podstrkuje falešné webové stránky, které uživatele přesvědčují k instalaci updatu pro Adobe Flash Player. Asi je zbytečné dodávat, že instalační soubor ve skutečnosti obsahuje virus.

Takové útoky se již dříve objevily v zahraničí – jako geograficky nejblíže by se mohl zmínit útok na zákazníky polské banky mBank, kde se majitelé napadených routerů přesměrovávali na falešné stránky tohoto peněžního ústavu s cílem získat jejich přihlašovací údaje.

Kde je problém?

Na různé zranitelnosti routerů třídy SoHo (Small office, Home office) už několik měsíců specialisté poukazují, takže v tomto směru nebyl tento útok až tak překvapivý (v případě TP-Linku podle prvotních poznatků mohlo jít o zneužití již déle známé zranitelnosti, které se říká ROM-0).

A ani výskyt potíží přímo v České republice – jde totiž o první oficiálně hlášený případ v tuzemsku – není nic, co by mohlo někoho šokovat.

Naopak tím, co experti neočekávali, je, že si všichni reportující, mezi nimiž byli často znalí lidé z IT komunity, byli naprosto jisti, že jejich router neměl dostupné konfigurační rozhraní přístupné přes síť WAN.

Na základě těchto informací se tedy očekávalo, že jde o jinou chybu jako například CSRF, která patří k dalším zranitelnostem ohrožujícím routery TP-Link, nebo třeba nějaký Javascript, který by se s webovou stránkou natáhl do prohlížeče a pak zkusil zaútočit na zranitelnost ROM-0 prostřednictvím rozhraní LAN routeru.

Csirt.cz podle svých slov nejdříve přes LAN otestoval, zda napadený kousek trpí zmiňovanou zranitelností ROM-0. Ta mimochodem spočívá v tom, že je možné z URL http://IP_adresa_routeru/ROM-0 stáhnout soubor, který po dekódování poskytne přihlašovací jméno a heslo ke směrovači.

Po ověření této zranitelnosti se pátralo dále – hledalo se, kde se v routeru zapíná a vypíná vzdálená správa přes WAN rozhraní. TP-LINK však tuto možnost nenabízel.

Muselo se tedy jít jinou cestou. Jeden z pracovníků centra si vzal router domů a připojil jej na svou linku s technologií ADSL namísto svého dosavadního směrovače. Pak zkusil zaútočit na ROM-0 zranitelnost prostřednictvím veřejné IP adresy přidělené k WAN rozhraní napadeného routeru. Atak se podařil úplně stejně jako předtím přes rozhraní LAN.

Je tedy jasné, že většina správců těchto řešení byla přesvědčena, že pokud na routeru není možnost zapnout vzdálenou správu přes WAN, pak zařízení tuto možnost vůbec nemá. Koho by napadlo, že je standardně povolená a nikde ani není jednoznačná volba pro její vypnutí?

Po tomto zjištění se začalo hledat řešení, které by útoku přes WAN rozhraní zabránilo, a zároveň se oskenovaly IP adresy přidělené do České republiky. Na nich specialisté Csirt.cz nalezli více než 5 000 routerů (nemusí jít o konečné číslo), které trpí pravděpodobně stejnou zranitelností, a útočník je tedy může zcela ovládnout.

Možná náprava

Pokud tedy ve své kanceláři či doma vlastníte ADSL modem/router, který má rok výroby mezi lety 2005 a 2013, nebo jej někomu spravujete, doporučuje se jej otestovat a případně udělat následující opatření.

Vzhledem k existenci zranitelnosti ROM-0, na kterou u některých výrobců ani neexistuje oficiální záplata, a protože k možným dalším zranitelnostem na starších routerech TP-Link, D-Link, Zyxel, Billion, ZTE i na dalších doporučují experti zcela zakázat přístup na webovou administraci z rozhraní WAN.

Pokud je to možné, povolte administraci pouze z jedné konkrétní vnitřní IP adresy. Zablokování se dá uskutečnit pomocí seznamů ACL (Access Control List), které je možné najít v nastavení Access Management.

Csirt.cz také upozorňuje, že zranitelností ROM-0 trpí mnoho typů zařízení různých výrobců, neboť se svazuje se systémem ZyNOS, který je sice produktem společnosti Zyxel, ale používá se i v zařízeních mnoha dalších výrobců.

Tyto klony od originálního kódu ZyNOS divergovaly, takže odpovědnost za zabezpečení odvozených výrobků už přechází na jejich konkrétní výrobce, kteří ale v některých případech nenaplňují běžné představy o kvalitě testování a podpory.

Pro rychlé otestování svého routeru ze strany WAN rozhraní lze navštívit webové stránky *http://rom-0.cz*, které provozuje sdružení CZ.NIC. Webový server umožňuje vykonat automatický test a případně upozorní na napadnutelný router. ■

Autor pracuje jako bezpečnostní analytik Národního bezpečnostního týmu Csirt.cz

Co může zneužít SoHo Pharming

Celý útok je mimořádně nebezpečný a podlý, protože postihuje všechna zařízení v síti bez rozdílu platformy a obchází standardně důvěryhodný DNS strom. Útočník může zajít tak daleko, že uživatelům, které nasměruje na falešné stránky nějaké služby, může servírovat obsah například podle operačního systému.

Uživatelům Windows tak může podstrčit falešný update pro Adobe Flash Player v podobě spustitelného (exe) souboru, zatímco uživateli mobilního telefonu s OS Android naopak aplikaci v podobě apk, která je nově „nezbytná“ pro používání dané služby z mobilního telefonu.

Možnosti zneužití jsou tedy opravdu vysoké, nejhorší však je, že díky hloupé souhře chyb ROM-0 a defaultně dostupné administrace přes WAN může tento útok postihnout i uživatele, kteří se o bezpečnost svých zařízení jinak dobře starají.

Zaujal vás tento příspěvek? Čtěte související články s příbuznou tematikou on-line.