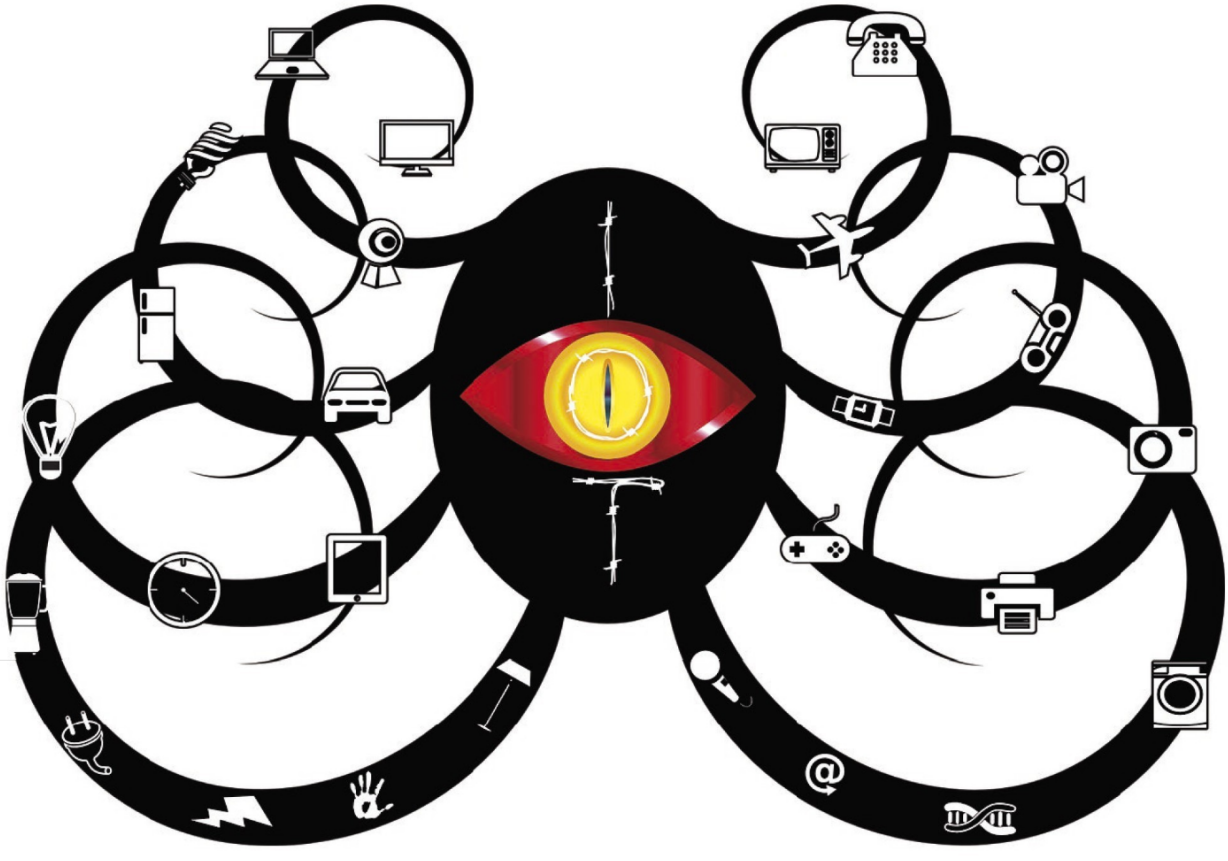
Prijetnja koja čuči i jača



Hajime (“početak”, na japanskom) je IoT crv koji se prvi put spominje 16. listopada 2016. u priopćenjima za javnost Rapidity Networksa, a prema ozbiljnim procjenama, do sada mrežu čini više od 300.000 uređaja. Prava mu je svrha i namjena još uvijek nepoznata, ali najvjerojatnije se radi o platformi za neki ozbiljan DDoS napad u skoroj budućnosti. Crv se stalno mijenja i razvija te su mu s vremenom dodane neke nove te uklonjene neke inicijalne funkcionalnosti

Rajko Plečko

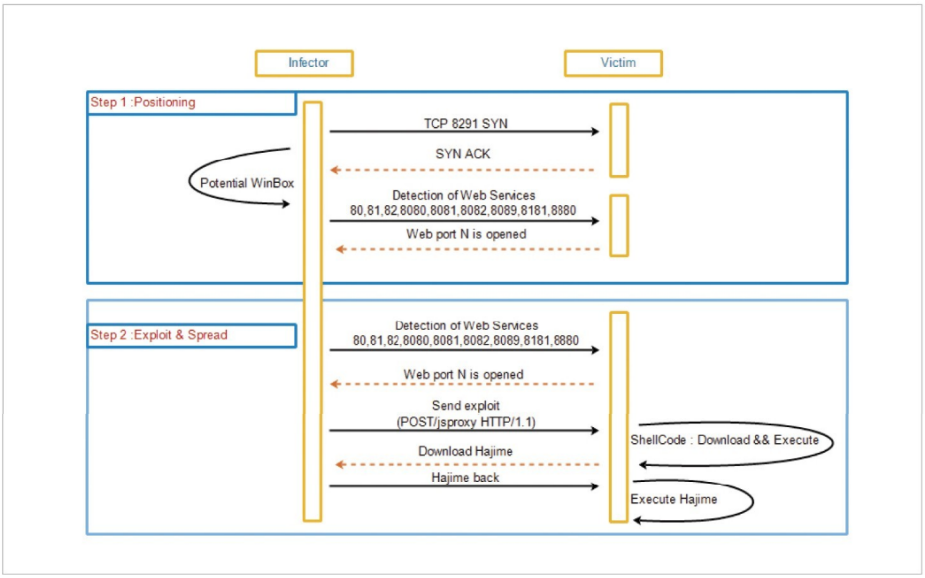
U posljednjih nekoliko tjedana sigurnosni stručnjaci iz cijelog svijeta primijetili su zanimljivo povećanje prometa prouzročeno skeniranjem Hajime IoT *botneta*, a usmjereno na masovnu "zarazu" nezaštićenih Mikrotikovih *routera*, naročito onih koji vrte neku od neažurnih verzija ROS-a (Router Operating System). Prema informacijama sa stranica Bleeping Computer, posvećenih računalnim, sigurnosnim i tehničkim pitanjima, napadači su pokušali iskoristiti ranjivost imanentnu verzijama ROS-a nižim od 6.38.4, koja je napadačima dopuštala izvršavanje zlo-ćudnog kôda i preuzimanje uređaja.

Ta ranjivost kodnog imena "ChimayRed" bila je spomenuta u Vaultu 7 WikiLeaksa kao jedan od hakerskih alata CIA-e, koji je proteklih godina često korišten za kompromitiranje Mikrotikovih *routera*. Čak i ako vam ne prouzroči veću štetu, taj incident svakako će vas podsjetiti na rasprostranjen problem ranjivosti uređaja povezanih na Internet, koji ih čine atraktivnim ciljevima hakera, koji ih žele iskoristiti u gradnji i širenju svojih IoT *botneta*.

ŠTO JE I KAKO NAPADA

Crva Hajime IoT otkrili su sigurnosni eksperti Rapidity Networksa u Coloradu, još u jesen 2016. godine. Kao i Mirai prije njega, Hajime se uglavnom oslanjao na ranjivost nezaštićenih uređaja, što je isključiva posljedica nemara, a to je zaboravljanje postavljanja lozinke na uređaje koji su u svojoj osnovi računala, ali im je namjena nešto drugo (web-kamere, *routeri*, DVR-ovi i slični). Takve uređaje napada sa zadanim korisničkim imenom i lozinkom na otvorenom Telnet *portu*, postavlja svoje pristupne podatke i zloćudni kôd te čeka aktivaciju, koja uglavnom pokreće neki masivni, ciljani DDoS napad. Takvi nezaštićeni uređaji predstavljaju ogromnu platformu za napadače, pružajući im potencijal da za svoje potrebe zauzdaju tisuće uređaja i pretvore ih u privatnu vojsku za napade iz čiste zabave ili, češće, prema narudžbi, uz nezanemarivu zaradu.

Kako se Hajime razvijao i mijenjao, razvijena je i metoda napada na Mikrotikov ROS. Sam pokušaj napada slijedi vrlo jednostavan uzorak. Uređaji zaraženi Hajimeom skeniraju nasumične IP adrese na *portu* 8921 (koji je na *routerima* uglavnom otvoren zbog administracije alatom WinBox), na temelju kojeg su uglavnom u stanju zaključiti da se radi o



Ovako izgleda tijek napada i inficiranje ciljanog sustava

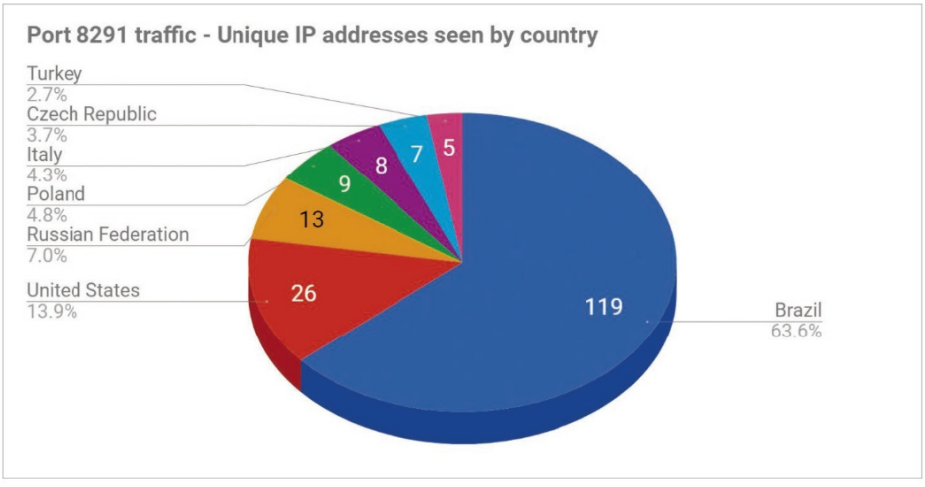
Mikrotikovom uređaju. Nakon inicijalne identifikacije, počinje ozbiljnija akcija inficiranja kroz ranjivost Chimay Red, gdje se pokušava "infekcija sustava" kroz jedan od *portova* na kojem bi eventualno mogao biti omogućen web-pristup (80, 81, 82, 8080, 8081, 8082, 8089, 8181, 8880). Nakon uspješne infekcije, inficirani uređaj postaje dio mreže i sam počinje skenirati IP adrese tražeći potencijalne žrtve.

KAKO SE OBRANITI

Kao što je vidljivo, Hajime za svoje širenje najvećim dijelom koristi propuste koje smo napravili prilikom konfiguracije *routera*, bilo zbog nemara ili neznanja, bilo zbog (pre) niske razine paranoje, koja je u primjerenoj dozi dobrodošla pri postavljanju zaštitnih mehanizama bilo kojeg uređaja ili sustava.

Već odavno jedan od važnijih uvjeta da bismo postali ciljem napada nije zanimljivost podataka kojima raspolažemo, jer je veći dio procedura automatiziran i dehumaniziran. Modernog napadača zanimaju naši resursi, koje bi mogao iskoristiti za svoje potrebe u nekom budućem napadu. To znači kako se ne bi smjelo dogoditi da na mreži imamo bilo kakav uređaj otvoren za pristup, a da nema postavljenu kompleksnu lozinku, i prema mogućnosti, izmijenjeno korisničko ime administratora.

Ako govorimo o Mikrotiku, na raspola-



Pita prikazuje rasprostranjenost izvora napada na jedan od sustava

"Uhvaćen" kôd napada

ganju nam je pregršt mogućnosti koje se međusobno ne isključuju nego izvrsno nadopunjuju. Prvo što bi trebalo napraviti jest redovito osvježavanje novim verzijama ROS-a, jer proizvođač na sve novootkrivene ugroze promptno reagira i u nove verzije unosi sve potrebne promjene i poboljšanja. Preporuka je svakako čuvati *backupe routera* i svaku novu verziju testirati i provjeriti – nije se jednom dogodilo da uz nekoliko poboljšanja dođe i poneki novi *bug*, ali to je jednostavno priroda stvari protiv koje ne možemo poduzeti gotovo ništa. Doduše, u takvom slučaju uvijek se možemo vratiti korak natrag, ako nam je ugrožena neka od važnijih funkcionalnosti. Ako nakon postavljanja jake lozinke i kreiranja novog administratorskog korisničkog računa onemogućimo "admina", koji je tvornički zadani administrator, prva linija obrane je postavljena.

MUDRO PREBACIVANJE

Ako ne koristimo web-administracijski alat (WebFig), svakako ga treba onemogućiti, a u slučaju da nam je potreban, mudro ga je prebaciti na neki od *portova* koji ne asocira na standardni (iz liste *portova* koje Hajime skenira vidljiva je sličnost i asocijacija na *port* 80). Loša strana odabira nekog visokog *porta* je u tome što nam se može dogoditi da s nekih (bolje štićenih) mreža nećemo moći ostvariti promet prema njemu. Također, ako si to možemo dozvoliti, mudro bi bilo onemogućiti i WinBox, ili ga u najmanju ruku preseliti na neki nasumični *port*, iako je to vjerojatno jedan od najboljih načina za administraciju *routera*. I tu se izlažemo riziku da takvom WinBoxu nećemo odasvud moći pristupiti.

Što nam je ostalo? Kad sve spomenuto pozatvaramo (Telnet smo, nadamo se, zatvorili još pri prvoj instalaciji *routera*) ostaje nam pristup SSH klijentom, koji nikako nije bez grijeha, ali je svakako najsigurniji. Treba li spomenuti da lozinke moraju biti dugačke, kompleksne i "negovoreće"?

Tu smo se, naravno, vratili na početak priče, odnosno na naredbeni redak, no žrtva kvalitete za poziciju u šahu je poznat koncept koji pritom treba imati na umu. Na raspolaganju su nam i još neki mehanizmi Mikrotikova *firewalla*, među kojima je "Adresna lista" jedan od jačih.

Kako? Kreiramo listu adresa s kojih bismo eventualno mogli pristupati svojem *routeru*. To mogu biti dvije-tri adrese ili, primjerice, sve adrese koje se koriste u Hrvatskoj (ako se ne bojite domaćih hakera). Nakon toga stvorimo pravilo koje zabranjuje pristup sa svih ostalih adresa, i eto nas još jedan korak dalje u zaštiti svoje mreže. Za ilustraciju količine neželjenog prometa, na *routeru* na kojem je zabranjeno sve osim hrvatskih IP adresa u manje od dva dana u filter je palo više od 1,5 GB prometa! Očigledno se ne radi o slučajnim prolaznicima, nego o gomili zaraženih uređaja koji konstantno traže ranjivosti. M

SAMO NEKI ALATI

Ovo nikako nije konačni set alata i rješenja, nego samo neke mogućnosti kojima u relativno kratkom vremenu možemo spriječiti da nam mali mlaz vode ispere cijelu branu. Za sveobuhvatnu listu metoda korisno je posjetiti Wiki stranice proizvođača koje se ovom problematikom bave do najsitnijih detalja. Kako se radi o vrlo velikoj i šarolikoj korisničkoj bazi, u potrazi za idejama i rješenjima nije na odmet konzultirati pripadajuće forume ili korisničke grupe na LinkedInu. Koju ćemo metodu odabrati i što ćemo sve kombinirati u naporima da se što bolje zaštitimo, na svakom je pojedinom administratoru, no najvažnije je probuditi svijest da apsolutna sigurnost ne postoji te kako je potrebno pratiti promete na uređajima i pokušati uočiti svaku eventualnu promjenu koja odskače od postavljenog *baselinea*, kako bismo na vrijeme mogli intervenirati. ◀