MIPS Router targeted Worm Botnet

With OpenWrt SDK Toolchains

Oleh: rizal.rasmalian@gmail.com

Abstrak

Mirai botnet bukanlah malware pertama yang menyerang peralatan ***IOT***. Namun, dengan di rilisnya source code Mirai botnet di internet, membuka peluang botnet – botnet baru bermunculan. Serangan botnet – botnet baru pun makin beragam, mirai botnet yang asli sendiri "hanya" menyerang service telnet pada port default 23 dan 2323 dengan sekitar 60 kombinasi default username dan password. Mirai botnet di klaim menginfeksi 2,5 juta peralatan, karna masih kurangnya aware terhadap peralatan IOT, dan membiarkannya menggunakan password default. Botnet – botnet versi baru yang muncul kemudian dan sampai sekarang mulai memakai Teknik – Teknik lain di samping bruteforce login telnet. Seperti penggunaan exploit 0-day pada device tertentu, juga bruteforce pada service lain seperti SSH. ***Openwrt*** adalah salah satu system operasi berbasis GNU/Linux yang banyak di gunakan pada router dengan architecture salah satunya **MIPS**. Secara default OpenWrt akan menggunakan Telnet dan/atau web based untuk kemudian mengaktifkan service **SSH**.

Dalam paper ini, kita akan membahas kemungkinan untuk membuat ***Botnet worm*** Mips dengan ***Openwrt SDK*** yang mampu melakukan serangan ke service telnet openwrt, dan jika sudah di matikan, secara otomatis akan mencoba brute force pada service SSH Openwrt tersebut, ***Botnet worm*** juga menggunakan beberapa ***exploit*** untuk menyerang device tertentu dengan system operasi selain openwrt yang memiliki bug,untuk melakukan infeksi lebih jauh. Teknik seperti ini pernah dunia lihat pada saat insiden ***worm morris*** pada 1988. Jika anda berencana membuat botnet/worm/malware pada IOT device, maka paper ini akan membantu memberikan anda gambarannya.

Pendahuluan

Sejak the great worm (morris worm) menginfeksi internet pada 1988, perkembangan worm dan malware mengalami banyak perubahan. Perubahan ini membawa dampak positif dan negatif. Dampak positifnya, morris mengedukasi pengguna internet bahwa efek dari kelemahan sebuah aplikasi atau menggunakan password yang mudah di tebak dapat menyebabkan kekacauan yang luar biasa pada jaringan internet. Dampak negatifnya, worm morris ini membuka mata hacker bahwan "hanya" dengan sebuah program , seseorang bisa mengendalikan hidup matinya internet.

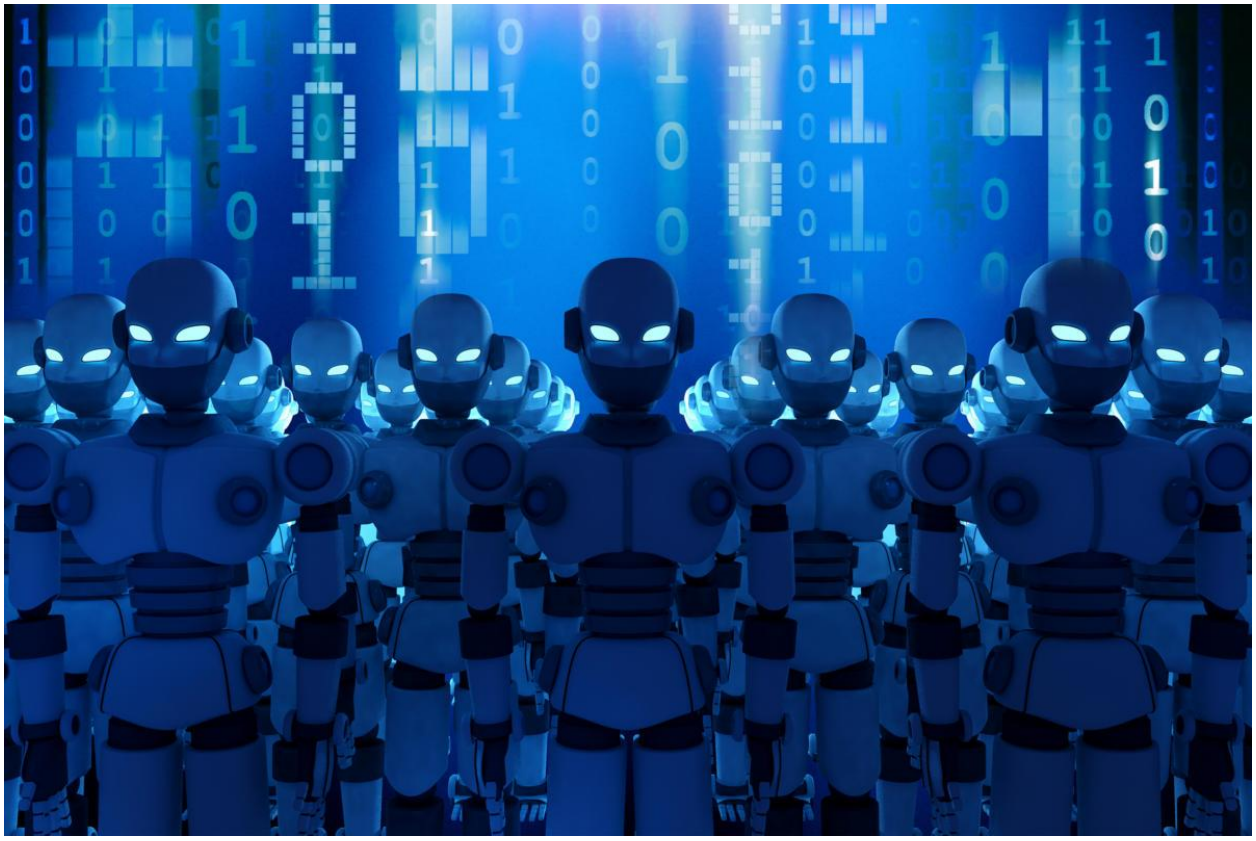
Sejak di rilisnya morris worm, banyak worm coder yang terinspirasi dari Teknik worm morris ini. Salah satu Teknik yang membedakan worm morris dengan Virus computer yang saat itu juga beredar adalah pada Teknik infiltrasinya. Dimana Worm morris ini, menyebar dengan cara otomatis tanpa campur tangan user, dengan memanfaatkan beberapa celah pada system operasi yang di serangnya. Selain itu Worm ini juga menyerang dengan Teknik brute force pada RSH / Rexec pada login – login dengan password yang biasanya di pakai.

Worm – worm tipe ini di kemudian hari juga berkembang menggunakan Teknik – Teknik lain yang di temukan pada system operasi modern seperti Windows , Linux (dan variannya) , web atau mungkin system operasi lain. Beberapa worm yang memanfaatkan celah keamanan, Sebut saja worm code red yang memanfaatkan celah Microsoft IIS Server. Juga ada worm SQLammer yang menyerang kelemahan Microsoft sql server, Worm Stuxnet yang lagi – lagi menyerang kelemahan system operasi Windows.

Pada 2016 ketika dunia IT sedang berkembang pada banyak aspek, dan memanfaatkan banyak gadget dalam kehidupan manusia, yang kemudian di kenal dengan sebutan IOT (Internet Of Things) muncul ancaman baru yang memanfaatkan configurasi yang lemah pada IOT Devices ini. Ancaman ini kemudian makin bertambah jumlahnya Ketika source codenya di rilis di internet, yang kemudian di kenal dengan IOT.Botnet Mirai . Mirai botnet ini mempunyai teknik yang hampir mirip dengan salah satu teknik Morris worm yaitu dengan melakukan brute force pada login telnet IOT Device,dimana seringkali menggunakan password default.

Mirai di golongkan sebagai botnet, meskipun dapat melakukan infiltrasi pada device IOT secara mandiri , namun loader Mirai pada device baru yang di infeksi di lakukan oleh server C&C (Command & Control). Selain itu,mirai di ketahui di manfaatkan untuk melakukan serangan DDOS pada banyak situs – situs berskala besar seperti twitter, Netflix, dan bahkan dyndns. Tingkat infeksi Mirai botnet varian original di perkirakan mencapai 2,5 juta device IOT. Serangan DDOS dengan Mirai botnet sendiri mencatatkan sejarah sebagai serangan DDOS dengan bandwidth terbesar sampai saat ini yaitu 1 Terabit per detik.

Dengan di rilisnya source code Mirai botnet, dunia menghadapi banyak varian mirai botnet yang beragam dan bahkan memanfaatkan banyak celah – celah yang di temukan pada IOT device, yang artinya varian – varian baru semakin canggih dan berbahaya.



Worm botnet kini makin canggih semenjak Mirai botnet menyerang internet, Teknik penetrasi makin canggih dan menggunakan exploit yang makin beragam, bahkan terakhir ada botnet yang menyertakan puluhan exploit sebagai senjatanya. Belum lagi jika membahas teknologi komunikasi antara botnet dan CNC yang mempunyai banyak perubahan sejak era mirai botnet. Belum lagi Teknik seperti mengintercept jaringan pada device tersebut,sehingga kemungkinan pencurian password penting bisa terjadi.

Kesimpulan

Dengan berkembangnya internet ke semua sector kehidupan, utamanya sejak pandemic covid-19 menyerang dunia, permintaan dunia akan device – device yang terhubung melalui internet juga makin banyak. Namun tentu saja, celah – celah baru juga di temukan dan di eksploitasi untuk penyebaran worm dan botnet di internet. Usahakan selalu mengikuti informasi bug /kelemahan keamanan terbaru di internet, karna mungkin saja bug tersebut mengenai device di rumah atau kantor anda.

Online presentation at IDSECCONF 2020 (Online) :

https://2020.idsecconf.org/p/registrasi.html