Abstrak

Deteksi DNS *Tunneling* dengan Elasticsearch

Protokol *Domain Name System* (DNS) merupakan media yang cukup populer yang digunakan oleh *malware* untuk melakukan *command and control* dalam mengendalikan komputer korban, teknik ini dinamakan sebagai DNS *tunneling*. Selain itu DNS *tunneling* juga dapat digunakan untuk *bypass captive portal hotspot* di tempat umum, dan memperburuk kualitas jaringan, namun yang lebih berbahaya adalah *eksfiltrasi* data melalui protokol DNS, protokol DNS yang seharusnya digunakan untuk mentranslasikan nama *domain*, dipergunakan untuk mengirimkan data, inilah kelemahan yang dimanfaatkan oleh penyerang untuk mengelabui Administrator jaringan. Pendekatan yang kami lakukan untuk permasalahan ini adalah dengan melakukan *traffic analysis* menggunakan *unique hostname* sebagai *indicator of compromise* dengan *tool* Elasticsearch untuk membantu Administrator jaringan dalam mengamankan jaringan dari DNS *tunneling.*

Dalam penelitian ini kami melakukan empat simulasi, yakni simulasi tanpa DNS *tunneling*, simulasi menggunakan *tool* Iodine, simulasi menggunakan *tool* Dnscat2, dan simulasi menggunakan *malware* DNSExfiltrator. *Output* deteksi DNS *tunnel* akan kami gunakan untuk memblokir DNS *tunnel* dengan DNS *sinkhole*. kami juga menguji kualitas jaringan untuk membuktikan apakah DNS tunneling mempengaruhi performa jaringan.

Hasil penelitian *traffic analysis* dengan menghitung *unique hostname* sebagai indikator terjadinya DNS *Tunneling* menggunakan Elasticsearch berhasil mendeteksi adanya kegiatan yang mengindikasikan terjadinya DNS *tunneling* dan dapat memberi notifikasi berupa *email* kepada Administrator Jaringan. Output nama domain dari hasil pendeteksian kami masukkan sebagai daftar blacklist DNS sinkhole, dan hasilnya nama domain tersebut tidak bisa melakukan DNS tunneling.

DNS *tunneling* dapat memperburuk kualitas jaringan tidak terbukti pada penelitian yang kami lakukan. Sehingga performa jaringan tidak bisa dijadikan sebagai indikator terjadinya DNS *tunneling*.

Kata kunci

DNS *tunneling*, data *exfiltration*, traffic analysis, Elasticsearch

Abstract

DNS Tunneling Detection using Elasticsearch

Domain Name System (DNS) protocol is a popular medium used by malware to do 'command and control' in controlling victim's computer, this technique called as DNS tunnelling. Furthermore, DNS tunnelling also can be used to bypass captive portal hotspot in public places, and worsen the network quality, more of that, it could be even more dangerous if DNS tunnelling is used for data ex-filtration through DNS protocol, a protocol which should be used to translating domain name, misused to transferring data. Those are weaknesses used by attacker to deceive the administrator. The approach we used to this problem is traffic analysis using unique hostname as indicator of compromise. To do that, we use a tool called Elasticsearch.

In this research, we do four simulations, the first one is simulation without DNS tunneling, the second is simulation using Iodine tool, the third simulation using DNScat2 tool, and the fourth simulation using DNSExfiltrator. The result of DNS tunnel detection we use to block the DNS tunnel using DNS sinkhole. We also test the network quality to prove whether DNS tunneling affect the network quality or not.

We successfully prove that the amount of unique hostnames is indicating the occurrence of DNS tunnelling. We do that using Elasticsearch tool. The tool is able to detect certain activity which is indicating the occurrence of DNS tunnelling. The tool is also able to notify the administrator via email. The domain name comes out from the detection can be listed in the DNS sinkhole blacklist, and the domain can no longer perform DNS tunnelling.

We conclude that DNS tunnelling does not worsen the network quality. So, the quality of the network cannot be used as indicator of DNS tunnelling.

Keywords

dns tunneling, elasticsearch, data exfiltration, traffic ananlysis