Cyberthreats – 3.2

#  DNS DDoS Attack Protections

* Resursele informationale afectate: Resursele afectate sunt: DDoS (distributed-denial-of-service) si CSPs (communications service providers)
* Prezentarea amenintarii : Raportul trimestrial Nexusguard, care se bazează pe date de la mii de atacuri DDoS din întreaga lume, a arătat că CSP-urile au fost vizate de 65,5% din atacurile DDoS întâlnite în T3 2018. S-a constatat că atacatorii au contaminat diverse grupuri de adrese IP în sute de Prefixe IP (cel puțin 527 de rețele de clasă C, conform constatărilor Nexusguard) cu trafic nedorit de dimensiuni foarte mici. Drept urmare, dimensiunea medie a atacurilor de la an la an în trimestru a scăzut cu 82%.

„Făptașii folosesc metode mai mici, fragmentare, pentru a injecta junk în traficul legitim, determinând atacurile să ocolească detectarea, mai degrabă decât să sune alarme cu vârfuri mari de atac evidente”, spune Juniman Kasman, director de tehnologie pentru Nexusguard. „Traficul difuz poate face ca furnizorii de servicii de comunicații să rateze cu ușurință atacurile DDoS la scară largă în curs de dezvoltare, motiv pentru care aceste organizații vor trebui să împartă încărcătura cu cloud-ul de la marginea rețelei pentru a minimiza impactul atacului”. a declarat Juniman Kasman, Chief Technology Officer pentru Nexusguard.

* Tipul amenintarii : DNS root
* Protagonistii amenintarii : Atacatorii de DNS-uri
* Masurile de securitate DDoS:
* Lățime de bandă suplimentară: O modalitate eficientă de a îmbunătăți protecția DDoS este creșterea lățimii de bandă disponibilă pe serverul web. Acest lucru permite serverului web să facă față creșterilor bruște și neașteptate ale traficului. Cu toate acestea, acesta este mai mult un tampon decât o soluție completă, oferind timp critic pentru a acționa înainte ca resursele dvs. să fie copleșite.
* Apărarea perimetrul rețelei:

- îmbunătățiți perimetrul de apărare al rețelei luând măsuri de securitate suplimentare, cum ar fi:

-limitarea ratei routerului pentru a preveni ca serverul web să nu mai răspundă la solicitări;

-aruncarea pachetelor falsificate sau malformate; și

-setați praguri mai mici SYN, ICMP și UDP.

-eliminarea întregului trafic: eliminarea unui întreg prefix IP poate fi o soluție, dar este costisitoare, deoarece va bloca și accesul la o gamă largă de servicii legitime.