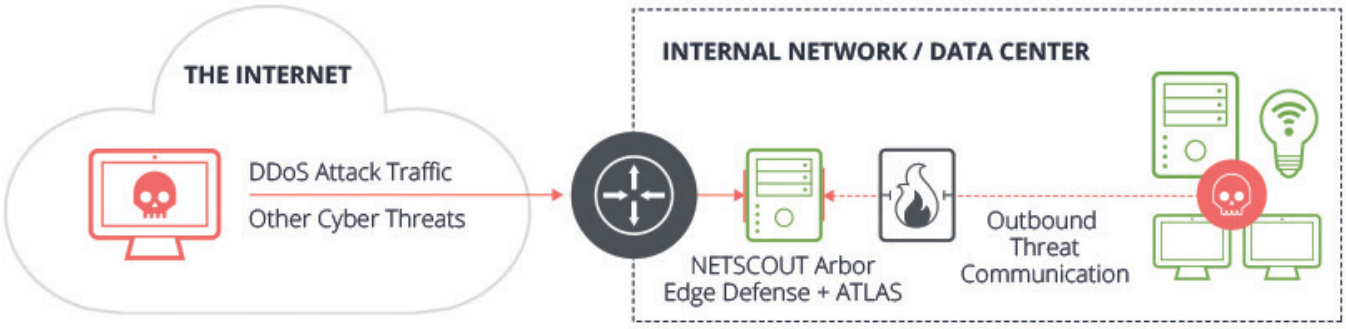
Arbor Edge Defense

Prva in zadnja linija zaščite pred naprednimi kibernetskimi grožnjami

.. Napadi DDoS niso nobena novost v svetu kibernetskih groženj. Danes smo namreč priča izrazito velikim napadom DDoS, ki dosegajo tudi vrednosti Tbps in pri katerih so večje tudi njihova moč, pogostost in kompleksnost ..



Avtorica: Ana Perkov

V takšnih napadih se običajno uporabljajo naprave IoT, sam napad pa je mogoče sprožiti s katerega koli mesta na svetu.

Niso pa samo grožnje DDoS tiste, proti katerim se moramo boriti. Vse večjo težavo predstavljajo napadi Advanced Persistent Threat (APT), napadi z izsiljevalsko programsko opremo, napadi z lažnim predstavljanjem, campaign threats …

Da bi se lahko organizacije zaščitile pred raznimi novimi grožnjami, ki se vsakodnevno pojavljajo, je sodoben varnostni sklad (angl. stack) postal večji in kompleksnejši, vendar žal še vedno zelo pogosto ne opravi svoje naloge dovolj kakovostno.

Letos je NETSCOUT predstavil nov izdelek, imenovan Arbor Edge Defense. Gre za rešitev "Beyond DDoS protection". Arbor Edge Defense – AED – uporablja edinstven položaj v omrežju in ga ščiti pred vsakršnimi dohodnimi in odhodnimi grožnjami.

Potrebna je več kot zaščita pred napadi

DDoS

AED je posebej usmerjen k zaščiti pred novimi spletnimi grožnjami. Eden izmed vzrokov za porast napadov je dvig ravni kompleksnosti omrežij. Napadalci napade nenehno izpopolnjujejo, v tradicionalne zlonamerne programske opreme dodajajo worm module, da bi zlonamerno programsko opremo čim hitreje razširili. Če se ozremo malce v preteklost in se spomnimo situacije NotPetya, kjer je bil (zlonamerni) program za dostop skozi skriti vhod (backdoor) vgrajen v priljubljen računalniški računovodski program, se je zlonamerna programska oprema iz osnovne tarče - Ukrajine, zelo hitro razširila po celem svetu.

AED zagotavlja zaščito obstoječih varnostnih rešitev

Tradicionalne varnostne naprave, nameščene na perimetru (zunanjosti) omrežja, kot so požarni zidovi Next-Gen, IPS ali rešitve load balancing, so podvržene napadom state-exhaustion. AED se postavi pred požarni zid ali rešitev IPS ter ju tako zaščiti pred napadom DDoS. AED uporablja stateless packet processing engine, ki zazna in ublaži veliko večino napadov DDoS brez spremljanja seje in njenega statusa. Kadar je treba zagotoviti spremljanje seje, AED shrani minimalno potrebne informacije o seji za kratek čas. Zaradi navedenega lahko AED prestane tudi ciljno usmerjene napade, katerih cilj je zapolniti tabelo sej na drugih izdelkih, s čimer ogrozi njihovo dostopnost in razpoložljivost.

AED blokira dohodne in odhodne grožnje

Omenili smo edinstven položaj, ki ga ima AED v omrežnem okolju in dodatno raven varnosti, ki jo nudijo zaščitni požarni zid ter rešitvi IPS/IDS. AED poleg tega blokira komunikacijo z znanimi sumljivimi destinacijami z uporabo seznama o ugledu aplikacije.

Za zagotovitev celovite zaščite pred grožnjami AED uporablja ATLAS – threat intelligence, ki so ga razvili inženirji v NETSCOUTU. AIF vključuje geolokacijske podatke in prepozna napade znanih botnetov in zlonamerne programske opreme ter zagotavlja redno in samodejno osveževanje baze groženj na sistemu AED prek varne SSL-povezave.

Učinkovita zaščita in sistem threat intelligence ne bosta prepoznala samo napada, temveč bosta zagotovila tudi zapise o celotnem napadu, da bi bilo mogoče lažje razumeti infrastrukturo, uporabljeno v napadu, metode in povezane pokazatelje. To bo olajšalo analizo in pospešilo ukrepanje, če do napada zares pride. Na ta način strokovnjaki za varnost dobijo širšo sliko in lahko veliko hitreje povežejo dohodni zlonamerni promet z odhodno komunikacijo ter hitreje odkrijejo ali prekinejo napade, preden je organizaciji povzročena nepovratna škoda.

Vas zanima demo predstavitev?

12.3.2019 podjetje Veracomp prireja dogodek, na katerem bodo predstavili omenjene rešitve.

Za več informacij pišite na arbor@veracompadria.com (P.R.)