Heuristika u ESET-ovim programima

Pitanje

- Što je heuristika?

Odgovor

U antivirusnom kontekstu, heuristika je skup pravila korištenih za detekciju sumnjivog ponašanja programa, bez potrebe za preciznom identifikacijom specifične prijetnje kao što je zahtijevano klasičnom detekcijom baziranom na virusnim potpisima.

Osim usporedbe potencijalnog malwarea prema poznatim virusnim potpisima, svi ESET-ovi programi koriste heuristiku za detektiranje virusa, trojanaca i ostalih prijetnji.
Primarna prednost modela baziranog na heuristici nije samo mogućnost detekcije različitih varijanti modificiranih formi postojećih malicioznih programa, već i otkrivanje potpuno novih i nepoznatih malicioznih programa. ESET Smart Security Premium, ESET NOD32 Internet Security i ESET NOD32 Antivirus koriste heuristiku da detektiraju i poznate i nepoznate prijetnje i malware. Koriste se dvije forme heuristike – pasivna i aktivna.

Pasivna heuristika

Pasivna heuristika analizira potencijalnu prijetnju kako je skenirana: kroz instrukcije u programu, prije propuštanja izvršnog koda procesoru na izvršenje. Pasivna heuristika traži uzorke, rutine ili programske pozive koji upućuju na maliciozno ponašanje. Iako je to važan alat, pasivna heuristika samo je dio rješenja, budući da nema ni jedne akcije koju provodi maliciozni program a da nije dopuštena i u legitimnom programu. To je razlog zašto je važna istodobna uporaba aktivne heuristike.

Aktivna heuristika

ESET-ova tehnologija aktivne heuristike kreira virtualno računalo unutar jezgre za skeniranje, što omogućuje skeneru da prati što bi ispitivani programski kod mogao napraviti ako mu se dopusti da radi na fizičkom računalu. To može otkriti potencijalno maliciozne aktivnosti koje druge tehnike detekcije ne mogu identificirati.

(posljednji puta revidirano 10.12.2018)
SOLN127