Veracomp d. o. o.

Trendi IT varnosti

..Kakšne nevarnosti prežijo na vaše IT sisteme?..

Avtor: Dejan Trop

Pred leti je bil tipični heker nekdo, ki je pozno ponoči sedel za svojim računalnikom in je načeloma napadal spletne strežnike in SQL baze, ki jih je našel na medmrežju, ter se poigraval z znanimi luknjami in pomanjkljivostmi v sistemu. Največkrat je kar zagnal skripto, ki je na medmrežju iskala računalnike z določeno ranljivostjo, ki jo je znal heker izkoristiti. Pogosto je bil njegov namen le raziskovanje in dokazovanje pred prijatelji. Če pa je tak heker naredil kaj nezakonitega, je to bila le trenutna prilika in nikakor ne vnaprej in skrbno načrtovani napad.

Toda časi so se spremenili.

Če bi želeli danes opisati tipičen hekerski napad, najprej ugotovimo, da gre za dobro organizacijo, pa s tem ne mislim samo na kriminalne združbe, za katerimi včasih stojijo hekerji, ampak mislim tudi na trg, na katerem se da danes prek temne strani interneta kupiti zlonamerno kodo, najeti botnete ali hekerja.

Največje grožnje, s katerimi se soočajo današnji IT varnostni sistemi

Kriminalne združbe

Kriminalne združbe v svojem osnovnem pomenu besede, kakor smo jih poznali do sedaj, so se ukvarjale s preprodajo drog, z igrami na srečo ali z izsiljevanjem, so sedaj dodale še kibernetski kriminal. Gre za dobro organizirane skupine, ki zaposlujejo svoje ljudi s polnim delovnim časom, imajo svoje kadrovske oddelke, skupine za vodenje projektov in vodje ekip. Znotraj teh organizacij imajo oddelek, ki se ukvarja z razvojem zlonamerne kode, oddelek, ki se ukvarja s trženjem, oddelek, ki se ukvarja z distribucijo itn.

Pralnice denarja

Obstajajo združbe, ki se ukvarjajo le s pranjem denarja, ki se nabira od kibernetskega kriminala. Te združbe se ukvarjajo s krajo identitet in gesel, da lahko preusmerjajo denar. Izvajajo goljufive transakcije s kreditnimi karticami, da pretvorijo pridobljena sredstva v gotovino. Te organizacije brez vprašanj izvajajo nedopustna gostovanja v državah, kjer jim roka pravice ne more nič. Na tak način takšne združbe vzdržujejo javne oglasne deske, 24-urno telefonsko podporo, vzdržujejo forume, nagrajujejo zveste stranke.

Hektivizem

Podjetja in organizacije se iz dneva v dan soočajo z naraščanjem števila organizacij, ki se združujejo z namenom političnega aktivizma. Najbolj znana skupina je Anonymous.

Hektivisti pogosto vnaprej napovedujejo svoje tarče in način napada na odprtih forumih, tako da lahko vsakdo izve, kdo bo napaden in s kakšnim razlogom. Večino svojih članov izberejo iz javnosti, in sicer ponavadi med tistimi, ki niso zadovoljni z aktualno politiko. Njihov namen je bolj, da spravijo napadalca v zadrego in da pridobijo medijsko pozornost. Največkrat se v zadnjem času poslužujejo DDoS napadov, saj s tem poskušajo povzročiti izgubo prihodkov napadenega.

Kraja intelektualne lastnine in podjetniško vohunnjenje

Vodilna in uspešna podjetja so pogosto tarča hekerjev, ki poskušajo pridobiti informacije oziroma načrte, zakaj in na kakšen način so ta podjetja uspešna. Cilj hekerjev je vdreti v podjetje, zbrati čim več gesel in čez čas ukrasti več gigabajtov podatkov, kot so na primer patenti, ideje za izdelke, vojaške skrivnosti, finančne informacije, poslovne načrte in podobno. Takšen napad traja dalj časa in poskušajo ga obdržati prikritega, dokler je le možno. Takšen napad imenujemo napredna obstojna grožnja in ga je težko odkriti.

Botnet kot storitev

Botnet dandanes ni namenjen več samo tistemu, ki ga je ustvaril. Danes lastniki botnetov omogočajo njihov najem na uro. Sedaj, ko je na medmrežju že ogromno naprav in računalnikov okuženih z botneti (več kot 10 milijonov se jih okuži vsak dan), je najem zelo poceni, kar pomeni, da je distribucija zlonamerne kode zelo preprosta in ni draga.

Zlonamerna koda vse v enem

Sofisticirana zlonamerna koda, ki je danes že vse v enem. Ne deluje le tako, da okuži uporabnika, temveč omogoča prodreti v spletne strani in okužiti še ostale uporabnike. Takšen tip zlonamerne kode pogosto komunicira z upravljalno konzolo, ki jo upravlja heker. Prek nje lahko heker nadzoruje širjenje zlonamerne kode in jo po potrebi prilagaja in spreminja. Zaščita na uporabnikovi strani ponavadi ne zaščiti žrtve, saj se napad izvede z zaupanja vredne spletne strani, ki jo je žrtev že večkrat obiskala.

Iščete rešitev?

Podjetje Veracomp vam lahko pomaga, da premostite težave na področju IT varnosti, in sicer smo distributer uveljavljenih in priznanih vendorjev, kot so: Arbor Networks, Extreme networks, Entrust, F5 Networks, Gemalto, Gigamon, Proofpoint, Symantec in Trend Micro. V Sloveniji sodelujemo skoraj z vsemi IT podjetji, tako da skrbimo za njihovo izobraževanje in jim nudimo popolno tehnično in prodajno podporo.

Vse končne stranke se na nas lahko obrnejo, ko potrebujejo svetovanje in pomoč pri odločitvi, katera rešitev bi bila za njih najbolj primerna. Seveda pa lahko pomagamo tudi tako, da v proces testiranja rešitve vključimo vendorja ali katerega od svojih poslovnih partnerjev. (P. R.)