Auteur: James Cheney, Technical Consultant, SRC Secure Solutions BV. James is te bereiken via jcheney@srcsecuresolutions.eu. Bewerkt en vertaald door SRC Secure Solutions B.V.

Geëmuleerde honeypots in de strijd tegen hackers

Honeypots worden al jaren gebruikt om aanvallers te lokken en te onthullen wie ze zijn, welke methoden ze gebruiken en hoe je moet reageren zonder de werkelijke bedrijfsmiddelen in gevaar te brengen. Door zich voor te doen als een server of ander waardevol aan het netwerk verbonden bedrijfsmiddel, lokt de honeypot aanvallers. De honeypot gebruikt fictieve gegevens, is geïsoleerd van het netwerk en wordt nauwlettend in de gaten gehouden voor het verzamelen van informatie.

Dit artikel beschrijft de geschiedenis van geëmuleerde honeypots en legt uit hoe geëmuleerde apparaten van allerlei aard kunnen dienen als valstrikken die veel verder gaan dan het verzamelen van informatie om cyberbeveiligingsteams te helpen een aanval op te sporen en tegen te houden.

Honeypots zijn het tegenovergestelde van conventionele beveiligingstools, die echte netwerkactiviteiten scannen en enorme hoeveelheden gegevens over activiteiten verzamelen. Honeypots zijn passief. Ze verzamelen geen gegevens over netwerkonderdelen, maar lokken aanvallers en verleiden ze tot het onthullen van informatie die tegen hen kan worden gebruikt.
Het honeypotconcept is al zo oud als de eerste echte computerhack, die Clifford Stoll gedetailleerd beschreef in zijn boek The Cuckoo's Egg. Stoll vertelt het verhaal van zijn jacht op een hacker die in 1980 inbrak in een computer van het Lawrence Berkeley National Laboratory (LBNL). Met behulp van Tymnet en verschillende overheidsinstanties ontdekte Stoll dat de inbraak via een satelliettelefoon afkomstig was van een universiteit in Duitsland en blijkbaar militaire bases als doelwit had om meer te weten te komen over het Strategic Defence Initiative (SDI), het Star Wars-project. Om de hacker over te halen zich bekend te maken, creëerde Stoll een primitieve honeypot - een fictieve afdeling bij het LBNL met een nepaccount van SDInet, vol met realistische en verleidelijke bestanden. Het daagde de hacker uit om dit systeem aan te vallen. De aanval werd getraceerd naar Markus Hess, die gestolen informatie verkocht aan de inlichtingendienst van de toenmalige Sovjet-Unie, de KGB.
Moderne honeypots maken gebruik van virtualisatie en AI om het gebruik ervan te vereenvoudigen. In deze blog noemen we ze 'honeypots met hoge interactie'. Hoewel ze moderner zijn dan de oorspronkelijke honeypots, zijn ze uiteindelijk conceptueel hetzelfde: kwetsbare middelen die zijn gebouwd om ervan te leren.

De noodzaak van misleiding

Of het nu gaat om sport, spel of oorlogsvoering, misleiding is essentieel voor elke succesvolle strategie. Het is duidelijk dat cyberaanvallers niet zonder misleiding kunnen. Als dat zo is, waarom is misleiding dan niet een steunpilaar in elk Security Operations Centre (SOC)? Misschien komt dat door het vroege succes en de reputatie van legacy honeypots. Het honeypotconcept heeft een imagoprobleem onder beveiligingsprofessionals die een verouderd idee hebben van het doel ervan. Velen beschouwen een honeypot als iets dat alleen geschikt is voor onderzoek op het gebied van cyberspionage, en zien ze daarom als geavanceerde extra's. Ten tweede brengt effectief gebruik van honeypots kosten en complexiteit met zich mee. Die beperken de mogelijkheden van een organisatie om honeypots op grote schaal in te zetten. Omdat het gebruik ervan in grote aantallen geen optie is, kunnen beveiligers ze niet verstoppen in een menigte. Daardoor kunnen honeypots alleen informatie verzamelen, en geen risico's beperken en systemen verdedigen. Het verouderde beeld van honeypots is een reëel probleem. Gezien de grote van het huidige doelwit, dat virtualisatie, cloud, IoT connected devices, shadow IT, werken op afstand en IT/OT-convergentie omvat. Ook al zijn virtuele honeypots eenvoudiger te implementeren dan fysieke, ze vereisen nog steeds isolatie, licenties voor de lokmiddelen, risicobeheer en monitoring.

Verborgen juweel

De honeypotgeschiedenis kent een verborgen juweel: de geëmuleerde honeypot. In tegenstelling tot een legacy honeypot, gebruikt een geëmuleerde honeypot geen werkelijke activiteiten om aanvallers te lokken. In plaats daarvan fungeert het als een normale asset, maar werkt het als een virtuele imitatie van een echt netwerk segment (inclusief servers en andere assets) . Aangezien de 'asset' virtueel is, is hij snel en eenvoudig in te zetten. En dan wordt het gebruik op grote schaal opeens een optie. Het doel ervan is om aanvallers te vangen, niet om ze te bestuderen.
Jammer genoeg vervagen door het grote aanbod de grenzen tussen legacy honeypots, geëmuleerde honeypots en lokmiddelen (valse bestanden, gegevens, enz.), waardoor organisaties denken dat ze de ene moeten kiezen boven de andere. Maar alle honeypots zijn waardevol als je ze op de juiste manier gebruikt. Hoe het ook zij, honeypots hebben een goed imago sinds hun uitvinding. Deze perceptie doet de unieke waarde van emulatie enigszins teniet.

Valstrikken - die een moderne versie van geëmuleerde honeypots zijn - zijn goedkoop en kunnen automatisch worden bewaakt, waardoor ze zeer praktisch zijn om snel en op grote schaal in te zetten.

Korte geschiedenis van geëmuleerde honeypots

De bekendste geëmuleerde honeypottechnologie is de opensourcesoftware Honeyd voor UNIX/Linux, die is ontwikkeld en wordt onderhouden door Neils Provos. Het kan verschillende besturingssystemen en diensten emuleren op TCP/IP-stackniveau. Het primaire doel van Honeyd is het detecteren van inbraken door alle ongebruikte IP-adressen in een netwerk tegelijkertijd te contro-

leren. Elke poging om verbinding te maken met een ongebruikt IP-adres wordt beschouwd als een ongeoorloofde of kwaadaardige activiteit. De eerste grote release dateert van 2003. Om dit in context te plaatsen: toen Honeyd werd gelanceerd, bestonden geavanceerde aanhoudende bedreigingen (APT's) nog niet. Evenmin als Facebook, LinkedIn, Gmail, iPhones of de cloud. Internet en telecommunicatie waren nog niet geconvergeerd. De IT-omgeving van vandaag de dag is heel anders en vraagt om een ander type geëmuleerde honeypot.

Geëmuleerde honeypots

Geëmuleerde honeypots worden ook wel medium interaction honeypots of traps genoemd). Deze honeypots hebben een IP-adres en zijn niet te onderscheiden van echte assets, maar zijn geen volledig uitgebouwde assets die licenties en computer en storage resources vereisen. In tegenstelling tot zuivere of traditionele honeypots die zijn gebouwd om te leren, zijn geëmuleerde honeypots gebouwd om aanvallers te vangen en bijvoorbeeld een sandbox omgeving in te sturen. Dit vereist slechts voldoende interactie om de aanvallers te identificeren en hun technieken te documenteren. Deze lichtgewicht en lowtouch benadering biedt unieke voordelen ten opzichte van honeypots met volledige interactie:

- Brede schaalbaarheid;
- Snelle inzetbaarheid;
- Laag risico voor dataverlies, omdat het geen echte, kwetsbare asset is;
- Agentloos;
- Ondersteuning voor operationele technologie (OT) en Internet of Things (IoT).

Geëmuleerde honeypots bieden nieuwe mogelijkheden voor misleiding. Hoewel het contra-intuïtief lijkt, kunt u hiermee risico's beperken door uw aanvalsgebied uit te breiden met vervalsingen. Het uitbreiden van het aanvalsgebied druist in tegen de conventionele cyberbeveiligingswijsheid, maar omdat de uitbreiding bestaat uit geëmuleerde assets is de strategie is zeer effectief.
Met emulatie kunt u nu groots inzetten en echte activiteiten verbergen. Organisaties met een volwassen beveiligingsbeleid dekken meer dan 30% van hun IP-portfolio af met geëmuleerde honeypots. Zij verminderen risico's door het waarschijnlijker te maken dat een aanvaller een valstrik zal raken dan een echt bedrijfsmiddel. Geëmuleerde honeypots zijn bij uitstek geschikt voor de bescherming van OT en IoT. Aangezien geëmuleerde honeypots agentless zijn, niet in contact komen met echte controllers en apparaten, en geen gevoelige informatie verzamelen, kunnen ze naadloos worden geïntegreerd in een productie-, energie- of gezondheidszorgomgeving, zonder de activiteiten te verstoren.

Geëmuleerde honeypots voldoen aan de meeste eisen voor misleiding, maar niet aan alle. Honeypots met een hoge mate van interactie (bijvoorbeeld volledige OS honeypots), met referenties, links en bestanden voorzien in een unieke behoefte en vullen geëmuleerde honeypots aan.

Opkomst van misleidingstechnologie

Miljoenen aangesloten apparaten (medische wearables, sensoren, controllers, slimme printers, camera's, koffiezetapparaten, thermostaten, speelgoed, geldautomaten, enzovoort) hebben een wirwar aan aanvalsmogelijkheden gecreëerd, waarvan cybercriminelen misbruik kunnen maken. Er zijn voorbeelden te over. De SolarWinds-aanval, met een zeer kleine malware-voetafdruk, die maandenlang onopgemerkt bleef, bewijst eens te meer dat aanvallers zich waarschijnlijk al in uw netwerk bevinden en weten hoe ze detectie kunnen vermijden;
Recente ransomwareaanvallen, zoals die op JBS Foods en Colonial Pipeline, maken duidelijk dat OT-netwerken gemakkelijke en lucratieve doelwitten zijn voor aanvallers.

De aanvallers van vandaag maken gebruik van aanvalstechnieken, waartegen conventionele beveiliging niet werkt. Veel aanvallen blijken onzichtbaar voor traditionele beveiligingstools, waardoor systemen en apparaten kwetsbaar zijn.
Moderne misleidingstechnologie met behulp van geëmuleerde valstrikken kan helpen dit nieuwe bedreigingsscenario te bestrijden. Ook binnen het actieve verdedigingsraamwerk Shield van MITRE speelt misleiding een sleutelrol in een modernere cyberbeveiligingsstrategie.
Misleidingstechnologie geeft cybercriminelen een vals gevoel van succes door hen te laten geloven dat ze voet aan de grond hebben gekregen in het netwerk. Deze truc geeft organisaties de tijd om op te treden tegen de aanvallers, terwijl de echte activiteiten worden beschermd.
De voordelen van deception technology zijn onder meer:

- Vroege detectie na een inbraak;
- Gemakkelijke schaalbaarheid (lage kosten en complexiteit);
- Laag risico voor de werkelijke activiteiten;
- Compatibiliteit met elk apparaat met een IP-adres.

Wat oud is, is weer nieuw

Het is tijd om geëmuleerde honeypots uit de beperkte context van de vroege jaren 2000 te halen en ze opnieuw toe te passen waar ze thuishoren: in het beveiligingslandschap van vandaag. IT/OT-convergentie, cloud en thuiswerken zijn het nieuwe normaal. Dekking van het aanvalsgebied met breed ingezette en aanpasbare misleiding is precies wat de dokter heeft voorgeschreven.