Honungsfällor

Att vilseleda och studera cyberangripare

Henrik Karlzén

FOI-R--5217--SE

December 2021

FOI

Henrik Karlzén

Honungsfällor

Att vilseleda och studera cyberangripare

Titel	Honungsfällor – Att vilseleda och studera cyberangripare
Title	Honeypots – Deceiving and studying cyberattackers
Rapportnr/Report no	FOI-R--5217--SE
Månad/Month	December
Utgivningsår/Year	2021
Antal sidor/Pages	35
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	Informationssäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr/Project no	E716527
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Bild/Cover: *Couch honeypot*, av Jean och Fred Hort. Från flickr.com/photos/jean_hort/5645617252 med licens https://creativecommons.org/licenses/by/2.0/

Sammanfattning

Den här rapporten beskriver grunderna om honungsfällor i cyberdomänen. En honungsfälla (eng. *honeypot*) definieras här som en cybersäkerhetsfunktion som med hjälp av vilseledning lockar till sig angripare och får dem att stanna kvar. Honungsfällor används för att förskona ägarens IT-system från angrepp samtidigt som lärdomar för framtiden kan dras om angreppen. Inom forskningslitteraturen finns dock ingen fullständig enighet om hur begreppet honungsfälla ska definieras.

Det finns många typer av honungsfällor och de kan delas in efter deras placering, nätverksroll, syfte, interaktionsnivå, samverkan, dynamik och omdirigeringsförmåga. Utöver honungsfällor finns det även liknande cybersäkerhetsfunktioner. Exempelvis rör det sig om tjärgropar (eng. *tarpits*) där angripare fördröjs samt en cybervariant av kamouflage.

Att använda honungsfällor är inte riskfritt. Om angriparen inte blir vilseledd har försvararen i bästa fall kastat bort sina pengar. I värsta fall kan angriparen vända på rollerna och börja vilseleda försvararen. En annan risk är att välvilliga utomstående upptäcker honungsfällan men utan att inse att den är en honungsfälla. Den utomstående kan då känna sig manad att rapportera den ovanliga aktiviteten som en incident vilket kan ge förvirring och skapa onödigt arbete. En tredje risk är att en angripare lyckas använda honungsfällan som språngbräda in i produktionsmiljön. Därtill finns det vissa frågetecken kring vilken användning av honungsfällor som är tillåten juridiskt.

Forskningen om honungsfällor har lett till att många olika honungsfällor tagits fram genom åren. Vad gäller mognaden hos dagens honungsfällor så är den tillräcklig för att möta enkla breddangrepp. Mognadsgraden är betydligt lägre vad gäller avancerade riktade angrepp. Honungsfällor har dock använts för att upptäcka tidigare okända sårbarheter (eng. *zero-days*).

Det finns potentiell nytta med att använda honungsfällor i en militär organisation som Försvarsmakten eftersom det finns stort behov av den typ av underrättelser och skydd som honungsfällor kan bidra med. Utöver nyttan finns dock också särskilda utmaningar med att använda honungsfällor i Försvarsmakten. Dessa utmaningar följer av att Försvarsmakten har en särskild hotbild och delvis ovanliga typer av IT-system. Försvarsmakten behöver därför göra en avvägning mellan honungsfällors potentiella nytta och den svårighet och risk som är förknippad med deras införande.

Nyckelord: honungsfälla, honungsnätverk, vilseledning, cybersäkerhet

Summary

This report describes the foundations of honeypots in the cyber domain. A honeypot is defined as a cybersecurity function that, with the help of deception, attracts attackers and gets them to stay. Honeypots are used in order to spare the owner's computer systems from attack, while learning lessons about the attacks for the future.

There are many types of honeypots, and they can be divided according to their placement, network role, purpose, interaction level, collaboration, dynamics, and ability to redirect. In addition to honeypots, there are also similar cybersecurity functions. For example, there are tar pits, where attackers are delayed, as well as a cyber-variant of camouflage.

Using honeypots is not risk-free. If the attacker is not successfully misled, the defender has at best wasted its money. In the worst case, the attacker can turn the tables and start deceiving the defender. Another risk is that a benevolent outsider discovers the honeypot, but without realizing that it is a honeypot. The outsider may then feel compelled to report the unusual activity as an incident, which may cause confusion and create unnecessary work. A third risk is that an attacker succeeds in using the honeypot as a springboard into the production environment. In addition, there are some questions about the legality of the use of honeypots.

The research on honeypots has led to many different honeypots being developed over the years. As for the maturity of today's honeypots, they are sufficient to meet simple unsophisticated attacks. The degree of maturity is significantly lower in terms of advanced targeted attacks. However, honeypots have been used to detect previously unknown vulnerabilities (zero-days).

There is potential benefit to using honeypots in a military organization such as the Swedish Armed Forces (SwAF), since there is a great need for the type of intelligence and protection that honeypots can provide. In addition to the benefits, however, there are also special challenges with using honeypots in the SwAF. These challenges follow from the fact that the SwAF is facing threats of a special type, and possesses partly unusual types of computer systems. The SwAF therefore needs to strike a balance between the potential benefits of honeypots, and the difficulty and risk associated with their introduction.

Keywords: honeypot, honeynet, deception, cybersecurity

Innehållsförteckning

1 Inledning

Den här rapporten beskriver grunderna om honungsfällor i cyberdomänen. En honungsfälla (eng. *honeypot*) är en cybersäkerhetsfunktion som med hjälp av vilseledning lockar till sig angripare och får dem att stanna kvar. Honungsfällor används för att förskona ägarens IT-system från angrepp samtidigt som lärdomar för framtiden kan dras om angreppen.

Det har forskats om honungsfällor i ungefär tjugofem år. Nyligen använde forskare ett hundratal honungsfällor för att under ett år simulera industriella system. Som forskarna väntat sig blev de simulerade systemen snart angripna och genom att studera angriparnas agerande upptäckte forskarna fyra dittills okända sårbarheter (*zero-days*) (Dodson m.fl., 2020). Honungsfällor har länge använts i praktiken för att skydda IT-system (nätverk, datorer, etc.) från angripare. I en mindre undersökning uppgav tjugo procent av de tillfrågade företagen att de använde honungsfällor, medan femtiotvå procent var villiga att använda honungsfällor (Neustar, 2019).

Det finns även intresse av honungsfällor inom den militära sfären. Exempelvis var honungsfällor en del av Natos övning Cyber Coalition 2020 (Tucker, 2020). Generellt har försvarsmakter större behov av underrättelser än vad de flesta andra organisationer har. Försvarsmakter behöver t.ex. kunna identifiera ihärdiga angripare och återkommande angreppstekniker för att strategiska beslut ska kunna tas och samhället som helhet skyddas. Det ökade behovet av underrättelser kan bland annat tillgodoses av honungsfällors möjliggörande av studier av angrepp.

1.1 Syfte och forskningsfrågor

Rapporten syftar till att öka kunskapen om honungsfällor bland de som vill försvara sina IT-system. Särskilt fokus är på att ge kunskap som kan användas för att göra avvägningar mellan honungsfällors nyttor och risker.

Följande forskningsfrågor besvaras:

1. Vad är en honungsfälla?
2. Vilka typer av honungsfällor finns?
3. Hur skiljer sig honungsfällor från andra säkerhetsfunktioner?
4. Vilka risker finns med att använda honungsfällor?
5. Är dagens honungsfällor mogna att ge praktisk nytta?

Rapporten har tagits fram i FOI-projektet *Analys av koncept och teknik för cyberförsvar och informationssäkerhet* vilket ingår i området *Operationer i cyberdomänen* i Försvarsmaktens samlingsbeställning inom forskning och teknikutveckling (FoT).

1.2 Metod

De källor som ligger till grund för rapporten har hittats genom explorativa sökningar i framförallt de akademiska databaserna Google Scholar och Scopus. Fokus har varit på akademiska forskningsartiklar och då framförallt de som redan har många citeringar av andra forskare. Även litteratur som är mindre formell förekommer dock i vissa fall som källor. Det rör sig i huvudsak om rapporter och böcker av forskare, texter från cybersäkerhetsföretag samt nyhetsartiklar.

I källorna finns många olika sätt att kategorisera material av de sorter som tas upp i denna rapport. Någon enskild vedertagen struktur finns inte och den struktur som används i rapporten kan ses som en kompromiss mellan olika möjliga strukturer.

1.3 Läsanvisning

Rapportens struktur är som följer.

Kapitel 2 ger olika möjliga definitioner av begreppet honungsfälla och mynnar ut i den definition som används i rapporten i övrigt.

Kapitel 3 tar upp olika typer av honungsfällor och kan ses som en informell taxonomi.

Kapitel 4 beskriver cybersäkerhetsfunktioner som är lika honungsfällor och var skiljelinjerna går.

Kapitel 5 redogör för honungsfällors risker.

Kapitel 6 tar upp vilka honungsfällor som finns och vad deras efterfrågan är samt vilken praktisk nytta honungsfällor kan ge.

Kapitel 7 diskuterar det som framkommit i rapporten.

2 Definition

Honungsfällor är den vedertagna översättningen av engelskans *honeypots*.[1] Det finns ingen fullständig enighet om hur begreppet honungsfälla ska definieras i cyberdomänen. Många (engelskspråkiga) forskningsartiklar hänvisar dock till någon av Spitzners definitioner, varav en fokuserar på honungsfällors syfte: *”en säkerhetsresurs vars värde ligger i att bli undersökt, attackerad eller kränkt”*[2] (Spitzner, 2002). Begreppet säkerhetsresurs (dvs. cybersäkerhetsfunktion) talar om ett väldigt övergripande syfte. I övrigt är det dock svårt att se att själva värdet med honungsfällor skulle vara att de undersöks, angrips eller skadas. Av liknande skäl är det tveksamt med det syfte som nämns i definitionen av Pouget m.fl. (2003): *”att observera intrång”*.[3] Ett mer naturligt syfte ges av Provos och Holz (2007, sid. xiv): *”att lära sig vilka sårbarheter som används av motståndare…eller vad en motståndare gör när den tagit över [systemet]”*.[4] Tallinnmanualen (Schmitt m.fl., 2013), vilken tagits fram inom ramen för ett Natosamarbete, nämner ett snarlikt syfte i form av att *”samla kontraunderrättelser om angriparen och dess angrepp”*.[5] Schmitt m.fl. (2013) nämner också ett kompletterande syfte: att *”slösa med angriparnas resurser”* (med meningslösa angrepp mot honungsfällan).[6] Detta syfte nämns även av Pouget m.fl. (2003). Men det är inte uppenbart att slösandet är ett värde i sig för försvararen. Ett mer naturligt syfte är att det riktiga produktionssystemet förskonas från angrepp. Kopplat till detta är det också möjligt att honungsfällan delvis utgör ett motvapen som kan infektera angriparen med skadlig kod (Wallace och Visger, 2018).

Det räcker inte att definiera honungsfällor utifrån deras syften eftersom syftena kan uppnås på många olika sätt varav vissa sätt normalt inte ingår i vad som benämns honungsfällor. Exempelvis kan lärdomar om angrepp och sårbarheter dras utifrån manuell kodanalys av skadlig kod, samtidigt som sådan kodanalys inte ingår i de metoder som honungsfällor brukar anses använda. Ett annat exempel är att vissa förskonande skydd finns i form av brandväggar, vilka inte räknas som honungsfällor. Honungsfällor behöver därför också definieras utifrån

[1] I Svenska Akademiens ordlista (2015) beskrivs ordet honungsfälla som ”något angenämt som kan leda till missbruk”, vilket dock inte stämmer med den definition som används i denna rapport.

[2] Fri översättning av *”A security resource whose value lies in being probed, attacked, or compromised”*.

[3] Eng. *”to observe intrusions”*.

[4] Fri översättning av *”To learn which vulnerabilities are being used by adversaries…or what an adversary does once he gained complete control over it”*.

[5] Sammanfattande översättning av *”gathering counterintelligence about the intruder’s intent, identity, and means and methods of cyber operation”*.

[6] Fri översättning av *”having the intruders waste resources [on the decoy environment]”*.

hur de uppnår sina syften. Med tanke på ordet honungsfälla ligger det nära till hands att anta att honungsfällor uppnår sina syften genom att locka angripare i en fälla med hjälp av ett lockbete (utlovad honung). Typiskt får angriparen aldrig lockbetet utan vilseleds bara. De lockande och vilseledande aspekterna inkluderas bland annat i definitionen i Tallinnmanualen (Schmitt m.fl., 2013). Även Fan m.fl. (2018) ser lockande som en essentiell del i en honungsfälla. Vad gäller vilseledning nämner Hirata m.fl. (2015) att det måste ske kontinuerligt för att inte angriparna ska upptäcka att de nått en honungsfälla snarare än det avsedda målet. För att lyckas med detta vilseledande måste honungsfällan i olika utsträckning påminna om det riktiga produktionssystemet, så att det finns lockbete efter lockbete. Honungsfällans likhet med produktionssystemet ökar också relevansen hos de lärdomar som kan dras av angriparens beteende.

Honungsfällor har alltså definierats både utifrån deras syften och utifrån den huvudsakliga metod som de uppnår syftena på. Det är därför rimligt att en ensad definition kombinerar dessa två aspekter. I den här rapporten definieras honungsfälla därför som följer:

En honungsfälla är en cybersäkerhetsfunktion som med hjälp av vilseledning lockar till sig angripare och får dem att stanna kvar, varpå ägarens IT-system förskonas från angrepp samtidigt som lärdomar för framtiden kan dras om angreppen.

3 Typer

Det finns många olika typer av honungsfällor. Vad som bedöms utgöra en egen typ beror på vilka aspekter honungsfällorna delas in efter. I forskningslitteraturen finns dock ingen vedertagen uppsättning av indelande aspekter. Exempelvis finns olika indelningar beskrivna av Joshi och Sardana (2011), Enisa (2012), Fan m.fl. (2018) samt Zobal m.fl. (2019). Det finns dock vissa aspekter och typer som återkommer i flera källor, även om ingen källa listar alla sådana vanliga aspekter och typer. Tabell 1 sammanställer de vanligaste typerna och aspekterna. I de kommande avsnitten ges mer detaljer om indelningen.

Tabell 1: Typer av honungsfällor indelade efter olika aspekter.

Aspekt	**Typ**
Placering	Internt Externt I DMZ[7] Uppdelat
Nätverksroll	Server Klient
Syfte	Forskning Produktionsskydd
Interaktionsnivå	Låginteraktiv Höginteraktiv
Virtualisering	Fysisk Virtuell
Samverkan	Enskild Honungsnätverk
Dynamik	Statisk Dynamisk anpassning efter nätverket Dynamisk anpassning efter angriparen
Omdirigering	Ingen Från gateway Från produktionssystem Från låginteraktiv till höginteraktiv

Det bör noteras att typerna (för en viss aspekt) inte nödvändigtvis är ömsesidigt uteslutande. Exempelvis kan en honungsfälla samtidigt vara till både för forskning och för produktion. Det bör också noteras att det finns kopplingar

[7] Demilitariserad zon (DMZ) är ett nätverk som ”separerar ett internt nätverk som är mer betrott från ett externt nätverk som är mindre betrott” (Akram m.fl., 2020).

mellan typerna (för olika aspekter), där vissa kombinationer är vanligare än andra. Exempelvis är dynamiska honungsfällor vanligtvis virtuella (Fan m.fl., 2018).

3.1 Placering

Honungsfällor kan delas in utifrån deras placering (Joshi och Sardana, 2011):

- *Internt*, i nätverket bakom brandväggen.
- *Externt*, i nätverket ut mot internet.
- *I DMZ*, mellan internt och externt nätverk.
- *Uppdelat*, dvs. med olika komponenter på olika platser.

Ett exempel på extern placering är spindelhonungsfällor (eng. *spider honeypots*), vilka skapar falska webbsidor som ligger och väntar på att så kallade spindlar ska leta sig igenom webbplatsen för att lära sig mer om den (Kaspersky, u.å.).

3.2 Nätverksroll

Honungsfällor kan delas in utifrån deras nätverksroll, beroende på vad honungsfällan agerar som (Enisa, 2012):

- *Server*.
- *Klient*, även kända som honungsklienter (eng. *honeyclients*).

Att agera som server kan också ses som att passivt vänta på att kunna samla in data, medan klientrollen kan ses som ett mer aktivt sätt att detektera skadligt beteende (se t.ex. Fan m.fl., 2018). Ikinci m.fl. (2008) beskriver på liknande sätt att honungsklienter är mer uppsökande än serverbaserade honungsfällor.

Serverbaserade honungsfällor är den vanligaste typen (Enisa, 2012; Fan m.fl., 2018). Det är också den typ av nätverksroll som denna rapport fokuserar på. Det är dock lämpligt att här ge honungsklienter visst utrymme. Honungsklienter kan exempelvis automatiskt surfa runt på webben för att upptäcka skadlig kod på olika webbplatser. Honungsklienter har beskrivits som särskilt svårtillverkade eftersom de måste klara av att hantera så många olika komplicerade och snabbföränderliga tekniker (Enisa, 2012). Dessutom är sannolikheten för falsklarm generellt sett högre än för serverbaserade honungsfällor, vilka generellt slipper falsklarm eftersom de saknar legitim användning (Enisa, 2012).

En snarlik indelning kan göras utifrån vilka tjänster och protokoll honungsfällorna imiterar (Zobal m.fl., 2019). Det kan till exempel röra sig om SSH, HTTP, FTP, Telnet, SMTP (Zobal m.fl., 2019), VoIP, IPv6 eller webbapplikationer (Fan m.fl., 2018). Det går också att dela in utifrån vad det övergripande användningsområdet är för det som efterliknas, såsom sakernas internet eller industriella kontroll- och styrsystem (Fan m.fl., 2018).

3.3 Syfte

Honungsfällor kan delas in utifrån deras övergripande syfte (Zobal m.fl., 2019):

- *Forskning,* dvs. syftet att studera angrepp.
- *Produktionsskydd,* dvs. syftet att skydda produktionsmiljön.

Ett urval av möjliga studieobjekt för forskningsfällor återges i Tabell 2 tillsammans med några källor.

Tabell 2: Vad honungsfällor kan studera hos angreppen enligt forskningslitteraturen.

Studieobjekt	**Källor som nämnt objektet**
Tekniker	Provos och Holz (2007); Fan m.fl. (2018); Crowdstrike (2021)
Sofistikation	Stech m.fl. (2016); Fan m.fl. (2018); Crowdstrike (2021)
Ihärdighet	Nawrocki m.fl. (2016)
Utnyttjade sårbarheter	Fan m.fl. (2018)
Ursprung	Nawrocki m.fl. (2016); Fan m.fl. (2018); Crowdstrike (2021)
Motiv	Stech m.fl. (2016); Fan m.fl. (2018)
Mål	Nawrocki m.fl. (2016); Crowdstrike (2021)
Konsekvenser	Fan m.fl. (2018)
Kringgående av säkerhetsfunktionerna	Pouget m.fl. (2003); Crowdstrike (2021)

Studierna ställer krav på att honungsfällorna kan skilja ut ett visst angrepp från annat som sker i honungsfällan. För de flesta serverbaserade honungsfällor (de som står och väntar på att bli angripna) finns inga legitima användare som exempelvis ändrar filer och därmed försvårar bedömningen av huruvida filförändringar är tecken på utpressningsvirus (eng. *ransomware*) (Provos och Holz, 2007). Falsklarm finns i större utsträckning för klientbaserade honungsfällor med tanke på att de är aktivt uppsökande (Enisa, 2012). Det kan också tänkas att en honungsfälla studerar flera angrepp samtidigt och att angreppen kanske då måste hållas isär. Att gruppera angrepp och angreppsdelar

har det bland annat forskats om i det franska Leurré-projektet (se t.ex. Thonnard och Dacier, 2008; Almotairi m.fl., 2008). Gruppering av angreppsdelar i angreppskedjor har det för honungsfällor även forskats om av Vasilomanolakis m.fl. (2016) samt för cyberangrepp i allmänhet om av Navarro m.fl. (2018).

3.4 Interaktionsnivå

Honungsfällor kan delas in utifrån deras möjliga nivå av interaktion med angripare (Mokube m.fl., 2007):[8]

- *Låginteraktiv* (eng. *low-interaction*), där angripare enbart kan interagera med simulerade tjänster snarare än ett riktigt operativsystem.
- *Höginteraktiv* (eng. *high-interaction*), där angripare kan interagera med ett riktigt operativsystem utan simulering.

Med högre interaktionsnivå följer större förmåga att vilseleda angripare (Enisa, 2012). Därtill ger en högre interaktionsnivå större möjligheter att studera angriparen och därmed samla in detaljerad angreppsinformation (Zobal m.fl., 2019). Å andra sidan ger en högre interaktionsnivå också negativa konsekvenser. Den högre interaktionsnivån ger större möjligheter för angriparen att agera på sätt som kan vara skadliga för försvararen, t.ex. om honungsfällan tas över och används som språngbräda för vidare angrepp (Zobal m.fl., 2019). Därtill kan det vara svårt att skilja angreppsdata från övrig information som genereras av vanliga godartade systemkomponenter i honungsfällan (Enisa, 2012). Dessutom är höginteraktiva honungsfällor mer besvärliga att ta fram och underhålla (Zobal m.fl., 2019). Tabell 3 sammanfattar egenskaperna för låginteraktiva respektive höginteraktiva honungsfällor.

Tabell 3: Egenskaper hos låginteraktiva och höginteraktiva honungsfällor.

Egenskap	Låginteraktiv	Höginteraktiv
Har hög vilseledningsförmåga	Nej	Ja
Genererar detaljerad angreppsinformation	Nej	Ja
Begränsar angriparen	Ja	Nej
Kan enkelt urskilja angreppsdata	Ja	Nej
Är enkel att ta fram och underhålla	Ja	Nej

Det finns många möjliga metoder och tekniker som kan användas för att upprätthålla interaktionsnivån i en honungsfälla. Exempelvis nämner Rowe (2019) många metoder. Några av dessa metoder kan sammanfattat återges som att en honungsfälla kan:

[8] En *mellaninteraktiv* variant nämns också av Mokube m.fl. (2007). Denna variant ligger mellan nivåerna låg och hög vad gäller interaktionsmöjligheten. Enisa (2012) benämner istället varianten som *hybrid*.

- Låtsas vilja utföra ett kommando men uppge att det inte går förrän ett lösenord uppgetts eller uppge att en annan användare stoppat kommandot.
- Leverera en efterfrågad fil men med en felaktig teckenkodning som gör filen mindre användbar.
- Uppge att ett kommando utförts fastän det inte gjorts.
- Ge ett felmeddelande.
- Simulera utförandet men efter en fördröjning.
- Låtsas som att angriparen utfört fel kommando och därför ge oväntade effekter.

Därtill föreslår Stech m.fl. (2016) att viktiga filer (t.ex. mejl och loggar) ersätts av fiktiva filer.

3.5 Virtualisering

Honungsfällor kan delas in utifrån deras virtualisering (Zobal m.fl., 2019):

- *Fysisk*, dvs. implementering direkt i en fysisk maskin utan virtualisering.
- *Virtuell*, dvs. implementering i en virtuell maskin eller annan virtuell miljö.

Den här aspekten är snarlik interaktionsnivån och alla honungsfällor med lägre interaktionsnivå kan ses som virtuella (Fan m.fl., 2018). Höginteraktiva honungsfällor använder däremot typiskt inte virtualisering (Urias m.fl., 2016). Det finns dock undantag där även höginteraktiva honungsfällor använder virtualisering. Fan m.fl. (2018) beskriver sådana undantag och vilka virtualiseringstekniker som då använts.

3.6 Samverkan

Honungsfällor kan delas in utifrån deras samverkan med varandra (Joshi och Sardana, 2011):

- *Enskild*, dvs. utan samverkan.
- *Honungsnätverk* (eng. *honeynet*), dvs. med samverkan.

Ett snarlikt sätt att dela in honungsfällor på är utifrån deras skalbarhet, dvs. möjligheten att enkelt införa fler honungsfällor (Fan m.fl., 2018).

Ett sätt att strukturera sina honungsfällor på är som minfält, vilket beskrivs av Fan m.fl. (2018). I denna struktur införs honungsfällor i relativt stora mängder och ofta vid nätverksperimetern varpå de bildar ett minfält. När angriparen tar kontakt blir angriparen automatiskt studerad (eller enligt liknelsen: sprängd).

3.7 Dynamik

Honungsfällor kan delas in utifrån deras dynamik (Fan m.fl., 2018):

- *Statisk*, dvs. utan dynamik.
- *Dynamisk anpassning efter nätverket*.
- *Dynamisk anpassning efter angriparen*.

En statisk honungsfälla väntar på att angriparen ska ge sig på just honungsfällan där den ligger och som den är konfigurerad. Statiska honungsfällor är vanligare än dynamiska (Tsikerdekis m.fl., 2018). Enisa (2012) nämner att i takt med att angrepp blir mer riktade, så blir det svårare att placera honungsfällor på ställen som kommer att nås av angripare. Resonemanget bygger på att riktade angrepp inte slår brett utan mer sannolikt hittar fram till produktionsmiljön (snarare än till honungsfällor).

En dynamisk honungsfälla kan uppnå sin dynamik genom automatisk anpassning till förändringar i miljön. Spitzner (2003b) beskriver att anpassningen möjliggörs av att nätverket lyssnas av passivt eller aktivt (med injektion av paket) varpå kunskap inhämtas om nätverket, maskinerna och deras tjänster. Detta medför att det på ett uppdaterat sätt kan avgöras hur honungsfällorna ska se ut för att smälta in i miljön samt hur många honungsfällor som är lämpliga. Fan m.fl. (2018) ger exempel på vad det behövs kunskap om, nämligen nätverkstopologi, operativsystem, tjänster och öppna portar.

En dynamisk honungsfälla kan också uppnå sin dynamik genom automatisk anpassning till angrepp. Pittman m.fl. (2020) beskriver vad de kallar för intelligensnivåer, vilka utgör olika nivåer av sådan dynamik. På lägre nivå kan honungsfällan inse att angriparen gör något allvarligt och då stänga av sig själv eller stänga ute angriparen. På en högre nivå kan honungsfällan härda sig själv utifrån tidigare angrepp. På högsta nivån kan honungsfällan ändra sig själv runt angriparen för att förbättra vilseledandet. Wagener m.fl. (2011) använder AI (i form av förstärkningsinlärning) för att lära sig angripares beteende i en honungsfälla. Kunskapen används för att exempelvis blockera program, byta ut program, eller förolämpa angriparen för att se vilket språk angriparen svarar på och om den alls svarar (dvs. huruvida angreppet sker automatiskt). Jiang och Xu (2004) beskriver hur nätverkstrafik kan övervakas för att identifiera vilka tjänster som för närvarande är attraktiva för angripare. Därefter införs honungsfällor med sådana tjänster. Det kan också noteras att dynamisk anpassning till angrepp även kan innebära att honungsfällan skapas vid behov när angrepp sker. Ett exempel på det beskrivs av Jiang och Xu (2004). Ett potentiellt problem med att anpassa sig efter angripare beskrivs av Obaidat m.fl. (2021). Om angripare är varse om anpassningen (dynamiken) kan den börja med att ge honungsfällan avsiktligt felaktiga tillvägagångssätt, varpå honungsfällan lär sig fel. Därefter är honungsfällan sämre redo för angriparens riktiga angrepp.

3.8 Omdirigering

Honungsfällor kan delas in utifrån deras möjlighet till omdirigering (flytt) mellan honungsfälla och andra enheter (Fan m.fl., 2018):

- *Ingen.*
- *Från gateway.*
- *Från produktionssystem.*
- *Från låginteraktiv till höginteraktiv.*
- *Från honungsfälla till produktionssystem.*

I vissa fall finns alltså ingen möjlighet till flytt.

I det enklaste fallet av flytt upptäcks misstänkt trafik redan i en gateway eller liknande och flyttas därmed över till en honungsfälla. Så är exempelvis fallet för honungsfällasystemet Potemkin (Fan m.fl., 2018). När denna typ av omdirigering kombineras med att ha flera honungsfällor samlade på ett ställe så används ibland benämningen honungsfarm (Yin m.fl., 2018).

I svårare fall har angriparen nått längre. Då måste flytten ske med hänsyn till det angriparen redan uträttat i angripen enhet. Sådana svårare fall beskrivs i resten av avsnittet.

Ibland finns det behov av att flytta angrepp från produktionssystem till honungsfälla. Ett exempel på hur det kan göras beskrivs av Urias m.fl. (2016). Det specifika produktionssystemet utgörs av ett mjukvarudefinierat nätverk (eng. *software-defined network, SDN*) med virtuella maskiner. När en virtuell maskin uppvisar ett suspekt agerande så används SDN:s flödesregler för att flytta maskinens TCP-anslutningar till en honungsfälla. Ett problem med flytt från produktionssystem är att angriparen inte ska märka att en förändring skett. Exempelvis kan förändringar i inloggningstillståndet i en webbapplikation avslöja honungsfällan (Hirata m.fl., 2015).

Ibland när låginteraktiva honungsfällor används visar sig honungsfällan vara undermålig för ett visst angrepp. Då vore det bra om angriparen kunde flyttas över till en höginteraktiv honungsfälla. Fan m.fl. (2018) beskriver två tekniker för omdirigering från en låginteraktiv honungsfälla till en höginteraktiv honungsfälla. Den ena tekniken är att förlita sig på flödesbaserad routning, som exempelvis i SDN. Den andra tekniken är att göra en överlämning av existerande TCP-sessioner. Ett problem med TCP-överlämning är dock att angriparen kan märka att IP-adress och MAC-adress ändrats. Att adresserna behöver ändras beror på att det annars skulle bli flera enheter i nätverket med samma adress och därmed svårighet att veta vilken enhet som ska ha vilken trafik. Sådana situationer är svåra att hantera om inte nätverket är av SDN-typ.

Ibland när flytt gjorts från produktionssystem till honungsfälla inser honungsfällan att beteendet trots allt är godartat. Då kan man vilja flytta tillbaka

till produktionssystemet. Ett sätt att utföra detta på beskrivs av Anagnostakis m.fl. (2005).

4 Relaterade säkerhetsfunktioner

Det finns flera cybersäkerhetsfunktioner som är lika honungsfällor och nedan ges exempel på sådana. Framförallt rör det sig om andra säkerhetsfunktioner som också vilseleder angripare. Beroende på den exakta definitionen av honungsfälla räknar forskningslitteraturen ibland de närliggande säkerhetsfunktionerna som honungsfällor.

4.1 Tjärgropar

Tjärgropar (eng. *tarpits*) utgör falska resurser i IT-system och fördröjer angripare (Oudot och Holz, 2004). Konceptet introducerades genom LaBrea som fördröjde angripare genom att sätta ett lågt TCP-mottagarfönster (eng. *receiver window*) för att därmed göra TCP-anslutningar väldigt långsamma (Provos och Holz, 2007). Ett annat praktiskt exempel är ett försvar mot utpressningsvirus (eng. *ransomware*) där försvararen förstorade filernas storlek för att angriparens kryptering av data aldrig skulle bli färdig (3ncrypt, 2019).

4.2 Nätverksteleskop

Nätverksteleskop (eng. *network telescope*) studerar trafik men håller sig till skillnad från honungsfällor passiva, snarare än att de interagerar med inkommande trafik (Enisa, 2012). Nätverksteleskop används exempelvis för att studera bakgrundsbruset på internet (Wustrow m.fl., 2010). Bakgrundsbruset, eller bakgrundsstrålningen, utgörs av trafik som sker till följd av felkonfigureringar eller breda skanningar efter sårbarheter (Pang m.fl., 2004). Ett exempel på ett nätverksteleskop är Caida som tar emot all trafik på ett /8-nät, dvs. ett nät som nås av 1/256 av alla internets IPv4-adresser (UCSD, u.å.).

4.3 Honungspolletter och honungssidor

Honungspolletter (eng. *honey tokens*) är lika honungsfällor men utgörs av mindre delar, såsom enstaka filer eller användarkonton (Pouget m.fl., 2003). Exempelvis kan särskilda användarkonton skapas som har osäkrare lösenord än de legitima användarkontona. Användarkontona utgör lockbeten för angripare och nyttjas i samband med övervakning för att angrepp tidigt ska upptäckas (Stech m.fl., 2016). En variant av honungspolletter är honungssidor, dvs. webbsidor som aldrig nås av normala besökare men som kan upptäckas av angripare vid deras kartläggningar. När angripare eller deras verktyg går in på sidorna får webbplatsens ägare en indikation om att angrepp pågår (Joshi och Sardana, 2011).

4.4 Kamouflage

En sorts motsats till honungsfällor är att se till att det riktiga systemet (felaktigt) ser ut som ett system som inte är intressant att angripa. Genom att ändra i systemens ytliga beteende kan försvararen se till att angriparen får en felaktig bild av systemen och deras egenheter (signaturer). Den felaktiga bilden gör att angriparen inte vill angripa, eller att angriparen lägger tid på att hitta intrångsverktyg mot fel typ av system (Albanese m.fl., 2015). Detta sätt att vilseleda motståndaren har inget vedertaget namn, men kallas i denna rapport kamouflage.

5 Risker

Det finns flera risker med att ha honungsfällor. Nedan beskrivs sådana risker som ofta nämns i forskningslitteraturen.

5.1 Honungsfällan upptäcks och vilseleds

En risk är att försvararen inte lyckas med att vilseleda en angripare. Särskilt svårt att upprätthålla vilseledningen blir det när angriparen aktivt letar efter avvikelser genom så kallad signaturigenkänning (eng. *fingerprinting*). Exempelvis kan angripare övervaka trafik för att se om det finns annan trafik än den som angriparen själv ger upphov till (Oudot och Holz, 2004). Angripare kan också undersöka hur honungsfällan svarar på särskilda förfrågningar, eller på korrupta paket (Fraunholz m.fl., 2017b). I de honungsfällor som testades av Enisa (2012) visade testerna inte på att någon av honungsfällorna hade skydd mot sådant.

Om angriparen inte vilseleds så har försvararen i bästa fall kastat bort sina pengar. I värsta fall kan angriparen vända på rollerna och börja vilseleda försvararen (Provos och Holz, 2007). Exempelvis kan angriparen skicka en stor mängd trafik till honungsfällan för att avleda försvararens uppmärksamhet, eller förse honungsfällan med felaktig information för att försvararen ska dra felaktiga slutsatser (Crowdstrike, 2021).

5.2 Honungsfällan upptäcks och rapporteras

En risk med att ha en honungsfälla är att välvilliga utomstående kan upptäcka den men utan att inse att den är en honungsfälla. Den utomstående kan då känna sig manad att rapportera den ovanliga aktiviteten som en incident till relevant instans. Det kan tänkas leda till förvirring och innebära onödigt arbete med att skapa klarhet hos de inblandade om att det inte rör sig om något illasinnat. Exempelvis beskriver Hilt m.fl. (2020) hur cybersäkerhetsföretaget Trendmicro hade en honungsfälla i ett system som för en cybersäkerhetsforskare såg ut som ett potentiellt angripet produktionssystem. Forskaren rapporterade därmed det hela till relevant myndighet för incidentrapportering.

5.3 Honungsfällan används som språngbräda

Honungsfällor har som IT-system i allmänhet typiskt någon form av teknisk barriär gentemot omvärlden. Exempelvis rekommenderar amerikanska standardiseringsorganet NIST att angrepp som studeras utan att stoppas bör

inneslutas i form av sandlådor, så att inte angripare kan kommunicera ut (Cichonski m.fl., 2012). För honungsfällor nämner Fan m.fl. (2018) möjligheten att omdirigera angripare till andra honungsfällor när angriparna försöker ta sig ut ur den första honungsfällan.

Om en angripare trots allt lyckas ta sig förbi barriären mellan honungsfällan och övriga system kan angriparen använda honungsfällan som språngbräda för vidare angrepp (Joshi och Sardana, 2011; Cichonski m.fl., 2012). Exempelvis beskriver cybersäkerhetsföretaget Trendmicro att en av deras honungsfällor utnyttjades av angripare för olika olämpliga eller bedrägliga aktiviteter (Hilt m.fl., 2020).

5.4 Juridiska problem

En risk med honungsfällor är att juridiska problem uppstår. Generellt är uppfattningen bland relevanta källor visserligen att honungsfällor är tillåtna. Det gäller exempelvis den Natorelaterade Tallinnmanualen (v 1.0, regel 61:2.c) (Schmitt m.fl., 2013). Därtill menar Radcliffe (2021) att juridiska implikationer inte bör avskräcka organisationer från att använda honungsfällor. Men potentiella juridiska problem är också något som ofta lyfts fram i forskningsartiklar om honungsfällor. En tidig analys var Salgado (2003) som utgick från amerikansk jurisdiktion. Den har ofta citerats och bedömdes av Sokol m.fl. (2017) som fortfarande viktig för det amerikanska perspektivet. Det bör noteras att de juridiska problemen med honungsfällor kan skilja sig åt mellan olika jurisdiktioner. Sokol m.fl. (2017) lyfter fram att sådana skillnader även kan finnas mellan olika medlemsstater i EU, och att det kan vara svårt att avgränsa sig till en specifik jurisdiktion med tanke på att cybersäkerhet är en global fråga där information delas över gränser. Det bör också noteras att det juridiska läget kan ändras snabbt, på grund av att lagar ändras eller tillkommer. De följande texterna om juridiska problem med användningen av honungsfällor bör därför tas mer som en utgångspunkt för specifika analyser än som ett allmängiltigt resultat. Indelningen av de juridiska problemen är snarlik den indelning som gjordes av Fraunholz m.fl. (2017a).

5.4.1 Ansvar vid motangrepp

Det kan vara lockande för försvararen att gå till motangrepp mot angriparen. Det är visserligen generellt tillåtet att försvara sig mot angripare men det är inte klarlagt att det är juridiskt tillåtet med motangrepp (på eng. ofta *hackback*) (Fraunholz m.fl., 2017a). Problemet är i huvudsak att motangreppet kan ge oförsvarbart stora skador på angriparen, eller rentav på tredje part (Fraunholz m.fl., 2017a). Juridisk analys har också gjorts för en mer passiv variant där försvararen infekterar honungsfällan med skadlig kod som senare kan infektera

och skada angripare (Wallace och Visger, 2018).[9] Källan utgår från att både angripare och försvarare är statsaktörer samt återger att majoriteten av Tallinnmanualens (Schmitt m.fl., 2013) experter anser sådan självinfekterad honungsfälla juridiskt riktig. Argumentet som majoriteten använde var att angriparen aktivt hämtade ut de infekterade filerna varför försvararen inte faktiskt skadade angriparen som istället hade sig själv att skylla. En minoritet av experterna hävdade dock att försvararen trots allt var ansvarig eftersom försvararen startade den händelsekedja som skadade angriparen.

5.4.2 Ansvar vid angrepp mot andra

Organisationer kan bli ansvariga (eng. *liable*) om de inte försvarar sina IT-system mot angripare som därmed tar över systemen och använder dem vid angrepp mot tredje part (Cichonski m.fl., 2012). Det är även möjligt att det kan röra sig om straffrättslig medhjälp att på detta sätt låta angripare använda ens system för att begå brott mot andra (Fraunholz m.fl., 2017a). Exempelvis kan brotten handla om lagring av stulen kreditkortsdata samt om distribuering av barnpornografi (Salgado, 2003).

5.4.3 Brottsprovokation och anstiftan

En angripare som kan visa att dess angrepp provocerats fram av polis (genom brottsprovokation, eng. *entrapment*) kan möjligen använda det som ett rättsligt försvar. Spitzner (2003a) och Radcliffe (2021) studerar i vilka situationer som honungsfällors lockande kan utgöra brottsprovokation i ett amerikanskt perspektiv. Utöver brottsprovokation kan det tänkas att försvararen blir ansvarig för anstiftan genom att ha frestat angriparen till att angripa. För tysk jurisdiktion menar Fraunholz m.fl. (2017a) dock att det vore osannolikt att försvararen skulle dömas eftersom angriparen redan tidigare haft som intention att angripa.[10] Å andra sidan kan underlåtenhet att försvara sin information göra att angripare inte kan dömas för brott. Så är bland annat fallet för företagshemligheter där brottsansvar bara kan komma på fråga om försvararen vidtagit rimliga åtgärder för att hemlighålla sin information.[11] Åtgärderna måste gå utöver att andra personer förstår att försvararen avsett att hemlighålla informationen.[12]

[9] Tillvägagångssättet påminner om att motverka incitamentet till stöld av ett klädesplagg genom att en bläckpatron satts fast på klädesplagget. Om patronen avlägsnas på fel sätt förstör bläcket klädesplagget.

[10] I normalfallet är det också svårt att se hur försvararen skulle kunna dömas för brott mot sitt eget system. Kanske äger försvararen systemet men har inte rätten att dela informationen med vem som helst. Fraunholz m.fl. (2017a) specificerar dock inte vilken typ av situation där anstiftan kan vara aktuell.

[11] Lag (2018:558) om företagshemligheter.

[12] Prop. 2017/18:200, sid. 31.

5.4.4 Personlig integritet

Ifall data om angripare utgör personuppgifter så måste försvarare hantera sådana data i enlighet med bestämmelser som rör personuppgifter (i EU framförallt dataskyddsförordningen, GDPR). Sådana data kan exempelvis utgöras av angriparens inloggningsuppgifter, IP-adress och nätverkstrafik (Sokol m.fl., 2017). Det finns visserligen situationer där t.ex. en IP-adress inte kan identifiera en person. Men eftersom det är svårt för försvararen att veta om det rör sig om en sådan situation så är det generellt lämpligt att betrakta IP-adresser som personuppgifter (i EU) (Sokol m.fl., 2017). Därtill menar Fraunholz m.fl. (2017a) att det enligt tysk rätt är tillåtet att publicera angripares ursprungsland, tid för ett angrepp och angreppets innehåll, men inte angriparens IP-adress eftersom det skulle kunna identifiera angriparen.

När personuppgifter trots allt måste behandlas kräver GDPR att det finns en rättslig grund med behandlingen. Den rättsliga grund som ligger närmast till hands för honungsfällor är intresseavvägning, dvs. att försvararen har ett intresse av behandlingen och att det intresset väger tyngre än angriparens rättigheter (Sokol m.fl., 2017).[13] Försvararens intresse är att skydda sig medan angriparens intresse exempelvis kan vara att dess IP-adress inte samlas in eller sprids. Sokol m.fl. (2017) argumenterar för att försvararens intresse väger tyngre än angriparens rätt till skydd för dess IP-adress. Detta ligger i linje med att tysk domstol bedömt det vara tillåtet att behandla IP-adresser i försvaret mot t.ex. överbelastningsangrepp och skadlig kod (Fraunholz 2017a). Liknande argument används i amerikansk kontext av Spitzner (2003a) som dock inte är övertygad om att argumentet kan användas för honungsfällor som används för forskning.[14]

I amerikansk jurisdiktion är det generellt förbjudet att övervaka elektronisk kommunikation. Undantag finns dock när den övervakade samtycker och för att inhämta samtycket är första steget att informera om intentionen till övervakning. Salgado (2003) och Spitzner (2003a) föreslår därför att angripare som tagit sig in i en honungsfälla möts av ett informationsmeddelande om att övervakning sker i systemet. Informationsmeddelandet avslöjar inte i sig att det rör sig om en honungsfälla, utan är likt de informationsmeddelanden som används i vanliga IT-system. Därtill menar Salgado (2003) att fortsatt användning av systemet kan ses som samtycke till att övervakning sker. Wallace och Visger (2018) föreslår liknande informationsmeddelanden, fast för att tala om att honungsfällan kan skada angriparen. Ett problem med informationsmeddelanden är dock att de inte kan visas överallt. Salgado (2003) föreslår därför att försvarare bara bör övervaka

[13] Punkten 49 i GDPR (EU-förordning 2016/679) nämner att intresseavvägning bland annat är relevant när syftet är att säkerställa nät- och informationssäkerhet (med vissa förbehåll). En annan rättslig grund som kan tänkas komma på fråga är att uppfylla lagkrav till följd av t.ex. säkerhetsskyddslagen. Det bör också noteras att myndigheter inte får använda intresseavvägning när de fullgör sina uppgifter. Istället ska grunden *allmänt intresse* användas.

[14] För forskning används normalt den rättsliga grunden *allmänt intresse*.

de portar i en honungsfälla som uppvisar informationsmeddelandet. Vad gäller EU-rätten ställer GDPR generellt krav på att den vars personuppgifter behandlas också informeras om behandlingen, och det oberoende av krav på samtycke. Vissa undantag för informationsskyldigheten finns dock, t.ex. om informerandet skulle göra det omöjligt eller avsevärt försvåra uppfyllandet av målen med behandlingen.

5.4.5 Upphovsrätt

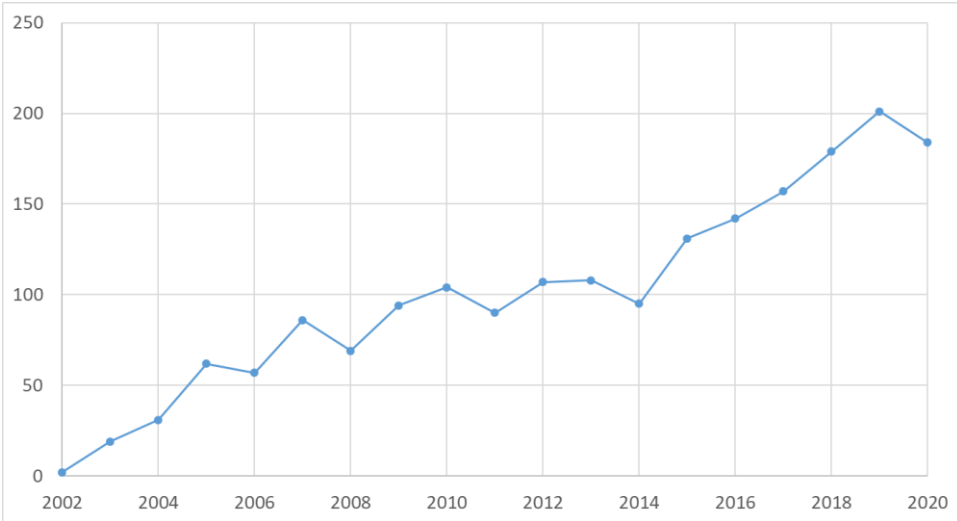
En försvarare som upptäcker ett angrepp vill förmodligen analysera de angreppsverktyg som angriparen fört in i systemet. En typisk analys består bland av dekompilering (en sorts reverse engineering) där maskinkod som är oläslig för människor kan översättas till mer lättförståelig källkod. Men sådana analyser kan begränsas av att angreppsverktygen typiskt omfattas av upphovsrätt (i EU) (Fraunholz m.fl., 2017a). Enligt EU-direktiv 2009/24/EG[15] är dekompilering förbjuden, annat än vad som krävs för att uppnå interoperabilitet och då bara för den som har rätt att använda programmet ifråga. Därtill kan upphovsrätten begränsa hur verktyget får kopieras, spridas, publiceras eller visas. I sammanhanget är det också relevant att angreppsverktygen kan vara mycket dyrbara, där en angreppskod (exploit) som utnyttjar tidigare okända sårbarheter kan vara värd miljoner (Fraunholz m.fl., 2017a). Men Fraunholz m.fl. (2017a) menar att angripare som använt egna verktyg förmodligen inte vill kräva sin rätt eftersom det också skulle innebära ett erkännande av angreppet. Å andra sidan nämner inte Fraunholz m.fl. (2017a) situationen där tredje parts verktyg använts vid angreppet.

[15] I Sverige införlivat genom lag (1960:729) om upphovsrätt till litterära och konstnärliga verk.

6 Mognad

De följande avsnitten beskriver tillgång och efterfrågan på honungsfällor samt vilken praktisk nytta honungsfällor ger. Nedan ges först en kort inblick i hur forskning om honungsfällor utvecklats över tid.

Forskningen om honungsfällor har växt stadigt de senaste två decennierna, enligt sökningen i forskningsdatabasen Scopus (genomförd 23 maj 2021 med sökströngen ”TITLE-ABS-KEY(honeypot*)”). Publiceringstakten är nu ungefär en ny forskningsartikel varannan dag.



Figur 1: Antal publicerade forskningsartiklar om honungsfällor per år.

6.1 Tillgång och efterfrågan

Forskningen om honungsfällor har lett till att många olika honungsfällor tagits fram genom åren. Nawrocki m.fl. (2016) beskriver 71 honungsfällor som togs fram under perioden 1997–2015. Många av dessa honungsfällor utvecklas och underhålls dock inte längre. Honungsfällorna underhölls i medeltal i 3,5 år och vid tiden för Nawrockis sammanställning underhölls fortfarande 20 av de 71. Bara sju har underhållits under perioden 2019–2021. De flesta är icke-kommersiella, men nio är kommersiella. Nedan beskrivs ett urval av de honungsfällor med öppen källkod som nämns av Nawrocki m.fl. (2016) och som fortfarande underhålls:

- Thug är en honungsklient i form av en (imiterad) webbläsare som surfar runt på olika webbplatser för att hitta de som angriper Flash, Adobe Reader och liknande (Nawrocki m.fl., 2016). Thug är den enda klientbaserade honungsfällan som Enisa (2012) rankade som essentiell för CERT:ar och dess kod nås på https://github.com/buffer/thug.
- Yalih är en liknande honungsklient som bland annat kan extrahera javascript-filer från webbplatser och sedan analysera filerna med mönsterigenkänning (Nawrocki m.fl., 2016). Samma källa nämner att Yalih dessutom kan samarbeta med mejlprogram för att besöka länkar i mejl och därmed kontrollera att webbplatserna som nås är säkra. Koden för Yalih nås på https://github.com/Masood-M/yalih.
- Conpot är en serverbaserad honungsfälla för industriella system och har förmågan att kommunicera via både internetprotokoll och vissa specifika industriella protokoll (Nawrocki m.fl., 2016). Dess kod nås på https://github.com/mushorg/conpot.
- Bluepot är en serverbaserad honungsfälla som tar emot skadlig kod via bluetooth och interagerar med olika bluetooth-angrepp (Nawrocki m.fl., 2016). Bluepot utvecklades ursprungligen som ett studentprojekt och koden nås på https://github.com/andrewmichaelsmith/bluepot.

Det finns också kommersiella honungsfällor. Två exempel på honungsklienter är Mcafees Siteadvisor och Microsofts Honeymonkey (Ikinci m.fl., 2008). För serverbaserade honungsfällor är ett exempel svenska Securiot som nås via https://securiot.se/products/securiot-honeypot-net. Honungsfällan kan enligt egen uppgift imitera industriella system, inklusive med MAC-förfalskning (eng. *spoofing*) (Securiot, 2021). I stället för att prata om honungsfällor pratar cybersäkerhetsföretag ofta om vilseledande teknik (eng. *deception technology*) (Rapid7, u.å.-b) eller vilseledningsplattformar (eng. *deception platforms*) (Palmer, 2018). Enligt nättidningen 3ncrypt (2019) var Rapid7 ett av de första företagen att tillhandahålla vilseledande cyberförsvarsteknik. Numera tillhandhåller Rapid7 en honungsfälla inbakad i en plattform (Rapid7, u.å.-a) som är gemensam med funktioner för loggverktyg, övervakning m.m. (Rapid7, u.å.-b). En konkurrent är Countercraft vars vilseledningsplattform (se Countercraft, 2021) användes i Natos cyberövning Cyber Coalition 2020 (Atherton, 2021).

Det är oklart hur stor efterfrågan på honungsfällor är. I en mindre undersökning uppgav tjugo procent av tillfrågade företag att de använde honungsfällor, medan femtiotvå procent var villiga att använda honungsfällor (Neustar, 2019). I en tidigare undersökning noterade Enisa (2012) att honungsfällor sågs som icke-essentiella säkerhetsfunktioner. Därtill noterar Tian m.fl. (2019) att honungsfällor inte används så mycket som försvar mot avancerade angrepp inom tillämpningsområdet cyberfysiska system.

Inom den militära sfären kan det noteras att Nato nyligen övat med honungsfällor (Tucker, 2020). Huruvida Nato använder honungsfällor skarpt ville dock inte

chefen för Natos cybersäkerhetscentrum svara på i en intervju i samband med övningen (ibid.).

6.2 Praktisk nytta

Nedan ges några exempel på hur honungsfällor gett nytta i praktiken:

- Amerikanska telekombolaget AT&T använde 2011 en honungsfälla för att upptäcka hur angripare tunnlade IPv6-trafik inne i IPv4-trafik med avsikten att undgå intrångsdetekteringssystem och brandväggar som inte anpassats för att förstå IPv6-trafik (Joshi och Sardana, 2011). Upptäckten ledde till ökad medvetenhet om vikten av IPv6-förståelse hos brandväggar och IDS:er.
- Ett hundratal av svenska Securiots honungsfällor användes nyligen av forskare för att simulera industriella system och på så vis dra till sig angripare (Dodson m.fl., 2020). Genom att studera angriparnas agerande upptäckte forskarna fyra dittills okända sårbarheter (*zero-days*).

Fler analyser kan ge mer praktisk nytta. För att underlätta sådana analyser tillhandahåller forskarna bakom honungsfällan IoTPOT sina insamlade data på https://sec.ynu.codes/iot. IoTPOT är en serverbaserad honungsfälla för telnet-angrepp mot sakernas internet (IoT).

Vissa källor i forskningslitteraturen menar att den praktiska nyttan hos dagens honungsfällor typiskt begränsas av att honungsfällorna är svåra att skapa och övervaka (Favre m.fl., 2017) samt konfigurera, implementera och införa (Urias m.fl., 2016). Det är dock oklart i vilken utsträckning dessa aspekter verkligen begränsar nyttan med honungsfällor. Exempelvis behövs mer kvantitativ validering av svårigheterna att implementera och underhålla honungsfällor (Pittman m.fl., 2020), även om vissa installations- och drifttester gjorts av Enisa (2012). Därtill är svårigheter med exempelvis konfiguration, implementation och införande generella problem i datornätverk snarare än specifika för honungsfällor (Urias m.fl., 2016).

7 Diskussion

Honungsfällor utgör en cybersäkerhetsfunktion som kan ta många former. En viktig egenskap hos honungsfällor är förmåga till vilseledning av angripare. Honungsfällors syfte är att locka till sig angripare för att förskona andra system från angrepp och för att dra lärdomar om angriparnas ursprung, metoder m.m. Mognaden hos dagens honungsfällor är tillräcklig för att möta enkla breddangrepp. Mognadsgraden är dock betydligt lägre vad gäller avancerade riktade angrepp. Därtill finns det vissa frågetecken kring vilken användning av honungsfällor som är tillåten juridiskt.

Det finns potentiell nytta med att använda honungsfällor i en militär organisation som Försvarsmakten. Där finns nämligen ett stort behov av den typ av underrättelser och skydd som honungsfällor kan bidra med. Det gäller till exempel att identifiera ihärdiga angripare och återkommande angreppstekniker för att strategiska beslut ska kunna tas och samhället som helhet skyddas.

Det finns också vissa särskilda utmaningar med att använda honungsfällor i Försvarsmakten. Dessa utmaningar följer bland annat av att Försvarsmakten har vissa ovanliga typer av IT-system. Många av Försvarsmaktens system är visserligen lika de som finns i civila organisationer, men det finns också system som använder speciell utrustning. Sådan utrustning kan vara särskilt svår att imitera i en honungsfälla.

Utmaningarna med att använda honungsfällor i Försvarsmakten följer också av den särskilda hotbilden. I hotbilden ingår visserligen vanliga angrepp som är enkla och oriktade, men också angrepp som är sofistikerade och riktade mot Försvarsmaktens specifika system. De mer sofistikerade angreppen utförs av angripare som är svåra att vilseleda. Svårigheten att vilseleda följer bland annat av att de avancerade angriparna har goda möjligheter att på förhand inhämta information om systemen. Exempelvis finns förmåga att värva insiders som kan ta reda på information om honungsfällor som statiskt placeras ut. För att trots allt kunna vilseleda dessa angripare krävs att realismen i honungsfällorna ökas samt att angriparnas underrättelseinhämtning hindras genom användning av mer dynamiska honungsfällor. Kompetenta och resursstarka angripare är dessutom svåra att hålla inkapslade i honungsfällorna. För att undvika att angriparna tar sig ur honungsfällorna och vidare till övriga system ställs därför särskilda krav på förmågan till separation.

Försvarsmakten behöver därför göra en avvägning mellan honungsfällors potentiella nytta och den svårighet och risk som är förknippad med deras införande. Förhoppningsvis kan denna rapport underlätta en sådan avvägning.

8 Referenser

3ncrypt. (2019). Beyond the honeypot: How military-inspired deception tactics are snaring cybercriminals. *Verdict.* https://verdict-encrypt.nridigital.com/verdict_encrypt_spring19/beyond_the_honeypot_how_military-inspired_deception_tactics_are_snaring_cybercriminals Besökt 14 juli 2021.

Akram, M., Barker, W.C., Clatterbuck, R., Dodson, D., Everhart, B., Gilbert, J., Haag, W., Johnson, B., Kapasouris, A., Lam, D., Pleasant, B., Raguso, M., Souppaya, M., Symington, S., Turner, P., Wilson, C. (2020). Securing Web Transactions: TLS Server Certificate Management. NIST Special Publication, 1800-16B. *National Institute of Standards and Technology (NIST).*

Albanese, M., Battistay, E., & Jajodia, S. (2015). A Deception Based Approach for Defeating OS and Service Fingerprinting. *IEEE Conference on Communications and Network Security.*

Almotairi, S., Clark, A., Mohay, G., & Zimmermann, J. (2008). Characterization of Attackers' Activities in Honeypot Traffic Using Principal Component Analysis. *IFIP International Conference on Network and Parallel Computing.*

Anagnostakis, K.G., Sidiroglou, S., Akritidis, P., Xinidis, K., Markatos, E., & Keromytis, A.D. (2005). Detecting targeted attacks using shadow honeypots. *Proceedings of the 14th conference on USENIX Security Symposium.*

Atherton, K. (2021). DIU Turns To Honeypots For Advanced Cyber Defense. *Breaking Defense.*

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. NIST Special Publication, 800–61. *National Institute of Standards and Technology (NIST).*

Countercraft. (2021). *CounterCraft launches the Cyber Deception Platform to detect, study and manipulate adversaries*. https://www.countercraftsec.com/blog/post/launch-cyber-deception-platform/ Besökt 14 juli 2021.

Crowdstrike. (2021). *Honeypots in Cybersecurity Explained*. https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/ Besökt 14 juli 2021.

Dodson, M., Beresford, A.R., & Vingaard, M. (2020). Using Global Honeypot Networks to Detect Targeted ICS Attacks. *12th International Conference on Cyber Conflict.*

Enisa. (2012). Proactive Detection of Security Incidents. Honeypots. *European Network and Information Security Agency.*

Fan, W., Du, Z., Fernández, D., & Villagá, V.A. (2018). Enabling an Anatomic View to Investigate Honeypot Systems: A Survey. *IEEE Systems Journal.*

Favre, O., Tellenbach, O., & Alsenzy, J. (2017). Honey-Copy – A Concept and Prototype of a Generic Honeypot System. *ICIMP 2017: The Twelfth International Conference on Internet Monitoring and Protection.*

Fraunholz, D., Lipps, C., Zimmermann, M., Duque Antón, S., Mueller, J.K.M., & Schotten, H.D. (2017a). Deception in information security: Legal considerations in the context of German and European law. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).*

Fraunholz, D., Zimmermann, M., & Schotten, H.D. (2017b). An adaptive honeypot configuration, deployment and maintenance strategy. *International Conference on Advanced Communication Technology, ICACT*, 53–57.

Hayatle, O., Otrok, H., & Youssef, A. (2012). A game theoretic investigation for high interaction honeypots. *IEEE International Workshop on Security and Forensics in Communication Systems*.

Hilt, S., Maggi, F., Perine, C., Remorin, Lord, Rösler, M., & Vosseler, R. (2020). *Caught in the Act : Running a Realistic Factory Honeypot to Capture Real Threats*. https://documents.trendmicro.com/assets/white_papers/wp-caught-in-the-act-running-a-realistic-factory-honeypot-to-capture-real-threats.pdf Besökt 14 juli 2021.

Hirata, A., Miyamoto, D., Nakayama, M., & Esaki, H. (2015). INTERCEPT+: SDN Support for Live Migration-based Honeypots. *4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security.*

Ikinci, A., Holz, T., & Freiling, F. (2008). Monkey-spider: Detecting malicious websites with low-interaction honeyclients. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*.

Jiang, X., & Xu, D. (2004). BAIT-TRAP: a Catering Honeypot Framework. *Purdue University*. https://friends.cs.purdue.edu/pubs/BaitTrap.pdf Besökt 14 juli 2021.

Joshi, R.C., & Sardana, A. (2011). Honeypots. A New Paradigm to Information Security. *Taylor & Francis.*

Kaspersky. (u.å.). *What is a honeypot?* https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot Besökt 14 juli 2021.

Mokube, I. Adams, M. (2007). Honeypots: Concepts, Approaches, and Challenges. *ACMSE*.

Navarro, J., Deruyver, A., & Parrend, P.A. (2018). Systematic Survey on Multi-step Attack Detection. *Computers & Security*.

Nawrocki, M., Wählisch, M., Schmidt, T.C., Keil, C., & Schönfelder, J. (2016). A Survey on Honeypot Software and Data Analysis. *ArXiv*. https://arxiv.org/pdf/1608.06249.pdf Besökt 14 juli 2021.

Neustar. (2019). *International Cyber Benchmarks Index. Latest survey results – March 2019.* https://www.niscicb.com/PreviousReports?view=2019%2Fmar Besökt 14 juli 2021.

Obaidat, M., Brown, J., Alnusair, A. Blind Attack Flaws in Adaptive Honeypot Strategies. *IEEE World AI IoT Congress.*.

Oudot, L., & Holz, T. (2004). Defeating Honeypots: System Issues, Part 1. *SecurityFocus.*

Palmer, N. (2018). The 'H' word. *Attivo networks.* https://attivonetworks.com/the-h-word/ Besökt 14 juli 2021.

Pang, R., Yegneswaran, V., Barford, P., Paxson, V., Peterson, L. (2004). Characteristics of internet background radiation. *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement.*

Pittman, J.M., Hoffpauir, K., Markle N., & Meadows, C. (2020). A Taxonomy for Dynamic Honeypot Measures of Effectiveness. *Arxiv*. https://arxiv.org/ftp/arxiv/papers/2005/2005.12969.pdf Besökt 14 juli 2021.

Pouget, F., Dacier, M., & Debar, H. (2003). Honeypot, Honeynet, Honeytoken: Terminological issues. *Institut Eurécom*. https://www.eurecom.fr/fr/publication/1275/download/ce-pougfa-030914b.pdf Besökt 14 juli 2021.

Provos, N., & Holz, T. (2007). Virtual Honeypots: From Botnet Tracking to Intrusion Detection. *Addison-Wesley Professional.*

Radcliffe, J. (2021). CyberLaw 101: A primer on US laws related to honeypot deployments. *SANS*.

Rapid7. (u.å.-a). *Honeypot.* https://docs.rapid7.com/insightidr/honeypot/ Besökt 14 juli 2021.

Rapid7. (u.å.-b). *InsightIDR.* https://www.rapid7.com/products/insightidr/ Besökt 14 juli 2021.

Rowe, N. C. (2019). Honeypot Deception Tactics. *Autonomous Cyber Deception*.

Salgado, R. (2003). The legal ramifications of operating a honeypot. I Spitzner, L. (2003). The Honeynet Project: Trapping the Hackers. *IEEE Security & Privacy*.

Securiot. (2021). *Securiot honeypot net.* https://securiot.se/products/securiot-honeypot-net/ Besökt 14 juli 2021.

Schmitt, M.N., red. (2013). Tallinn manual on the international law applicable to cyber warfare. *NATO Cooperative Cyber Defence Centre of Excellence.*

Schmitt, M.N., red. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd edition. *NATO Cooperative Cyber Defence Centre of Excellence*.

Sokol, P., Misek, J., Husak, M. (2017). Honeypots and honeynets: issues of privacy. *EURASIP Journal on Information Security*.

Spitzner, L. (2002). *Honeypots: Tracking Hackers.* Addison-Wesley.

Spitzner, L. (2003a). *Honeypots: Are They Illegal?* Securityfocus.

Spitzner, L. (2003b). *Dynamic Honeypots.* Securityfocus.

Stech, F.J., Heckman, K.E., & Strom, B.E. (2016). Integrating Cyber-D&D into Adversary Modeling for Active Cyber Defense. *Cyber Deception: Building the Scientific Foundation.*

Svenska Akademiens ordlista. (2015). Honungsfälla. *Svenska Akademien.* https://svenska.se/saol/?id=1132139&pz=7 Besökt 14 juli 2021.

Thonnard, O., & Dacier, M. (2008). A framework for attack patterns' discovery in honeynet data. *Digital Investigation.*

Tian, W., Ji, X.P., Liu, W., Zhai, J., Liu, G., Dai, Y., & Huang, S. (2019). Honeypot game-theoretical model for defending against APT attacks with limited resources in cyber-physical systems. *ETRI Journal.*

Tsikerdekis, M., Zeadally, S., Schlesener, A., & Sklavos, N. (2018). Approaches for Preventing Honeypot Detection and Compromise. *Global Information Infrastructure and Networking Symposium*.

Tucker, P. (2020). NATO Experiments With Deceptive Tactics to Lure Russian Hackers. *Defense One.* https://www.defenseone.com/technology/2020/11/nato-experiments-deceptive-tactics-lure-russian-hackers/170248/ Besökt 14 juli 2021.

UCSD. (u.å.). *The UCSD Network Telescope*. https://www.caida.org/projects/network_telescope/ Besökt 14 juli 2021.

Urias, V.E., Stout, W.M.S., & Lin, H.W. (2016). Gathering threat intelligence through computer network deception. *IEEE Symposium on Technologies for Homeland Security.*

Vasilomanolakis, E., Srinivasa, S., Garcia Cordero, C., & Mühlhäuser, M. (2016). Multi-stage attack detection and signature generation with ICS honeypots. *IEEE/IFIP Network Operations and Management Symposium.*

Wagener, G., State, R., Engel, T., & Dulaunoy, A. (2011). Adaptive and Self-Configurable Honeypots. *12th IFIP/IEEE International Symposium on Integrated Network Management.*

Wallace, D., & Visger, M. (2018). The Use of Weaponized “Honeypots” under the Customary International Law of State Responsibility. *The Cyber Defense Review*.

Wang, K. (2005). Using Honeyclients to Detect New Attacks. *RECON*. https://recon.cx/2005/recon2005/papers/Kathy_Wang/Wang-Honeyclients-RECON.pdf Besökt 14 juli 2021.

Wustrow, E., Karir, M., Bailey, M., Jahanian, F., & Huston, G. (2010). Internet background radiation revisited. *Proceedings of the ACM SIGCOMM Internet Measurement Conference.*

Yin, W., Zhou, H., Wang, M., & Jin, Z. (2018). A Honeyfarm Data Control Mechanism: Design, Implementation, Evaluation and Forensic Study. *IJCSNS International Journal of Computer Science and Network 8 Security.*

Zobal, L., Kolar, D. & Fujdiak, R. (2019). Current State of Honeypots and Deception Strategies in Cybersecurity. *Proceedings of the 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops.*

Den här rapporten beskriver grunderna om honungsfällor i cyberdomänen. En honungsfälla (eng. honeypot) definieras här som en cybersäkerhetsfunktion som med hjälp av vilseledning lockar till sig angripare och får dem att stanna kvar. Honungsfällor används för att förskona ägarens IT-system från angrepp samtidigt som lärdomar för framtiden kan dras om angreppen. Inom forskningslitteraturen finns dock ingen fullständig enighet om hur begreppet honungsfälla ska definieras.

Det finns många typer av honungsfällor och de kan delas in efter deras placering, nätverksroll, syfte, interaktionsnivå, samverkan, dynamik och omdirigeringsförmåga. Utöver honungsfällor finns det även liknande cybersäkerhetsfunktioner. Exempelvis rör det sig om tjärgropar (eng. tarpits) där angripare fördröjs samt en cybervariant av kamouflage.

Att använda honungsfällor är inte riskfritt. Om angriparen inte blir vilseledd har försvararen i bästa fall kastat bort sina pengar. I värsta fall kan angriparen vända på rollerna och börja vilseleda försvararen. En annan risk är att välvilliga utomstående upptäcker honungsfällan men utan att inse att den är en honungsfälla. Den utomstående kan då känna sig manad att rapportera den ovanliga aktiviteten som en incident vilket kan ge förvirring och skapa onödigt arbete. En tredje risk är att en angripare lyckas använda honungsfällan som språngbräda in i produktionsmiljön. Därtill finns det vissa frågetecken kring vilken användning av honungsfällor som är tillåten juridiskt.

Forskningen om honungsfällor har lett till att många olika honungsfällor tagits fram genom åren. Vad gäller mognaden hos dagens honungsfällor så är den tillräcklig för att möta enkla breddangrepp. Mognadsgraden är betydligt lägre vad gäller avancerade riktade angrepp. Honungsfällor har dock använts för att upptäcka tidigare okända sårbarheter (eng. zero-days).

Det finns potentiell nytta med att använda honungsfällor i en militär organisation som Försvarsmakten eftersom det finns stort behov av den typ av underrättelser och skydd som honungsfällor kan bidra med. Utöver nyttan finns dock också särskilda utmaningar med att använda honungsfällor i Försvarsmakten. Dessa utmaningar följer av att Försvarsmakten har en särskild hotbild och delvis ovanliga typer av IT-system. Försvarsmakten behöver därför göra en avvägning mellan honungsfällors potentiella nytta och den svårighet och risk som är förknippad med deras införande.

FOI

ISSN 1650-1942

www.foi.se