W16D4 - Ricerca di gruppo bonus: honeypot

Lavoro del gruppo NetRaiders a cura di Maria Zanchetta, Simone Malinverno, Daniele Zoccheddu e Tommaso Virgini.

Definizione di "honeypot" e breve storia.

Un honeypot è un sistema software o hardware progettato con delle vulnerabilità specifiche in grado di attirare gli hacker malevoli, che fa parte di una strategia di difesa in grado di individuare, ingannare e deviare dei criminali informatici. Vengono imitati in modo efficace dei servizi, delle web app o degli interi sistemi in modo da trarre in inganno gli attaccanti e studiare i loro metodi di attacco, valutando al tempo stesso le vulnerabilità del sistema per migliorare la difesa e la sicurezza. Gli attaccanti pensano di aver ottenuto l'accesso al sistema e di aver rintracciato dei dati utili, ma si tratta di un sistema isolato dal resto della rete, senza dati sensibili e controllato in modo da rilevare ed identificare l'attività degli hacker. Si tratta a tutti gli effetti di un'esca, del resto gli honeypot sono definiti speso come "decoy systems". Si ha a che fare quindi con una trappola che distrae gli hacker malevoli, protegge le reti e i dispositivi effettivamente sensibili ed aiuta a fermare i criminali informatici, studiando a fondo le loro mosse e migliorando la difesa degli asset importanti. Sebbene vi siano sistemi semplici in grado di registrare qualche dato o solo di lanciare un alert, grazie ad honeypot più elaborati è possibile rintracciare l'indirizzo IP di un attaccante e la sua posizione, specie se non vengono usate delle protezioni come una VPN, la password e in ogni caso vengono rilevate le modalità di accesso utilizzate, che consentono di studiare come affinare le difese contro futuri attacchi. Il termine "honeypot" deriva da un contesto militare di spionaggio e si rifà ad una trappola, magari anche romantica, che trae in inganno spie o nemici per poi monitorarli o costringerli a rivelare le loro vere intenzioni e si ispira al concetto del miele che attira le api. L'utilizzo di honeypot rientra nell'ambito della threat intelligence, per cui si osserva il comportamento e si studiando le tecniche di un attaccante in un ambiente controllato, mentre l'hacker porta avanti l'attacco contro un obiettivo che sembra possa dare accesso a dati importanti. Gli honeypot solitamente imitano sistemi o servizi vulnerabili, come un servizio basato su connessioni SSH oppure un browser che trova siti web che tendono ad eseguire dei payload malevoli. Le vulnerabilità scelte per gli honeypot sono semplici da sfruttare ma non troppo ovvie, in modo che gli attaccanti pensino davvero di aver sfruttato una vulnerabilità reale per entrare nel sistema target. Le funzioni degli honeypot verranno analizzate dettagliatamente in seguito, ma si possono riassumere con la raccolta di informazioni per individuare attacchi e studiarli a fondo, la necessità di migliorare la sicurezza dei sistemi grazie allo studio di attacchi e minacce reali e la possibilità di fare ricerca e limitare i crimini informatici. Possono essere piazzati nella rete interna, per trovare minacce già penetrate nella rete interna magari grazie al movimento laterale, oppure nella DMZ, ossia demilitarized zone, per trovare delle minacce esterne che cercano di entrare nella rete interna, o ancora possono essere integrati con un SIEM (Security Information and Event Management) per centralizzare l'analisi dei dati e le decisioni in caso di intrusione. Il primo honeypot è descritto nel libro di Clifford Stoll "The Cuckoo's Egg" del 1989, che parla di una trappola usata per rintracciare un hacker tedesco che cercava di violare i computer

militari statunitensi e che rappresenta un primo tentativo di studiare i comportamenti di un hacker tramite una trappola. Il primo Deception Toolkit di Fred Cohen è stato introdotto nel 1997, mentre nel 1998 è stato lanciato CyberCop Sting, ovvero il primo honeypot commerciale che segna il passaggio da un periodo di sperimentazione ad un uso più strutturato di questi strumenti. I primi honeypot simulavano semplici servizi come Telnet o FTP e sono diventati con il tempo sempre più complessi.

Finalità difensive e funzionamento.

Come verrà spiegato successivamente, gli honeypot sono strumenti molto versatili in grado di bloccare un grande numero di minacce informatiche. Possono catturare dei malware di vario tipo, che vengono poi analizzati e vanno ad aggiornare i database di firme, per esempio, degli antivirus e possono anche rilevare attacchi brute force, specialmente quando vengono imitati servizi come SSH ed RDP. Le credenziali utilizzate sono utili per individuare gli attaccanti e capire quali credenziali sono deboli e vulnerabili. Gli honeypot sono efficaci anche contro le botnet e verranno citati in seguito dei casi concreti, ad esempio contro la Mirai botnet, e riconoscono le prime avvisaglie di attacchi DDoS, evitando che poi l'attacco vero e proprio venga lanciato. Individuano anche exploit kits per attacchi con XSS oppure SQL injection e varie forme di reconnaissance scanning. Esistono varie tipologie di honeypot, ma si possono individuare degli step comuni nel loro funzionamento. Per prima cosa imbrogliano gli attaccanti, spacciandosi per servizi, sistemi o dispositivi legittimi e risultano molto attrattivi per portare avanti attività malevole di vario tipo, avendo delle vulnerabilità da sfruttare. Quando un attaccante compie qualche azione, partono i sistemi di monitoraggio e di logging per registrare cosa fa l'attaccante e raccogliere dati preziosi e vengono raccolti anche malware ed altri tipi di dati o comunicazioni. A questo punto vengono allertati gli esperti di cybersecurity, che possono decidere di analizzare i dati raccolti o possono implementare delle misure di sicurezza a protezione dei sistemi veri e propri.

Classificazione ed accorgimenti di sicurezza.

Esistono varie tipologie di honeypot e si possono classificare in base al livello di interazione con l'attaccante o in base allo scopo ed ambito del loro utilizzo. Per quanto riguarda lo scopo e l'ambito di utilizzo di questi strumenti, una prima classificazione riguarda gli honeypot di ricerca e gli honeypot di produzione. I primi vengono utilizzati per scopi di ricerca da enti di ricerca, professionisti della cybersecurity ed istituzioni per studiare varie tipologie di attacco ed affinare le tecniche di difesa. Un honeypot famoso è Dionaea, sviluppato come honeypot open source per scopri di ricerca nell'ambito di The Honeypot Project, che emula servizi presi di mira dagli hacker come http, SMB ed FTP e che ha dato un contributo importante in termini di ricerca per capire il comportamento degli attaccanti ed elaborare difese migliori. Un altro honeypot utilizzato per fini di ricerca è Glastopf, specializzato nel simulare web applications ed altre vulnerabilità sulla rete ed implementato per studiare vulnerabilità come XSS oppure SQLi. Gli honeypot di produzione, invece, vengono utilizzati dalle aziende o da altri enti privati e fanno parte di sistemi complessi di difesa, come possono essere gli IDS, ovvero Intrusion Detection Systems. È molto frequente trovare gli honeypot negli IDS,

perché gli IDS solitamente prevedono un'esca, come l'honeypot che attira gli hacker, un sensore che raccoglie informazioni, una console che monitora la rete e i dispositivi e un motore che analizza i dati raccolti e studia come migliorare la sicurezza. Gli honeypot servono proprio ad attirare l'attenzione degli hacker, tenendoli impegnati per un tempo sufficiente a raccogliere informazioni sull'attaccante, evitando che l'attaccante si renda conto di essere caduto in una trappola. Un famoso honeypot di produzione è Cowrie, creato da Michael Oosterhof, che imita un server Telnet e delle interazioni SSH ad alto livello e capace di raccogliere informazioni dettagliate in caso di attacco. Un altro esempio interessante è l'honeypot Canary. Esistono poi tre tipologie di honeypot classificati in base al livello di interazione con gli attaccanti, ovvero gli honeypot a bassa interazione, gli honeypot a media interazione e gli honeypot ad alta interazione. Gli honeypot a bassa interazione consentono solo un'interazione parziale con i sistemi, poiché offrono servizi con funzionalità ristrette e riproducono solo alcune parti del sistema che deve essere protetto, solitamente le parti più ambite ed interessanti per gli attaccanti. Essi sono più semplici da gestire e sono indicati per attacchi automatici e non sofisticati, come potrebbero essere bot e worm, ma non sono adatti per fronteggiare attacchi complessi portati avanti da attaccanti esperti. Questi potrebbero rendersi conto velocemente del fatto di essere in presenza di un honeypot e potrebbero cessare gli attacchi rapidamente senza lasciare informazioni preziose per chi deve difendere i sistemi. Questo tipo di honeypot emula solo i comandi basi di un protocollo, come SSH, per esempio viene presentata solo una finestra di dialogo di accesso usata per raccogliere nomi utenti e password e per un honeypot di questo tipo basta solo riprodurre i protocolli TCP ed IP e alcuni servizi di rete. Un esempio di honeypot a bassa interazione è Glutton, uno strumento molto versatile e facile da gestire in grado di accettare connessioni su ogni porta. Altri honeypot a bassa interazione sono Honeyd e LaBrea. Gli honeypot a media interazione sono più complessi perché imitano più parti del sistema ed offrono più comandi, basti pensare al software Cowrie che simula un filesystem completo ed offre comandi come netstat che fanno pensare agli attaccanti di essere veramente entrati nel sistema target. Possono anche simulare delle web app senza però riuscire ad imitare un intero sistema operativo e un esempio di honeypot a media interazione è Kippo, scritto in Python e che registra attacchi brute force e riproduce una vera e propria shell Linux con tutti i comandi. Questo honeypot è stato sviluppato Rey Juan Carlos University di Madrid e simula un server SSH che registra i comandi degli attaccanti, registra le loro azioni ed offre uno spazio sicuro per l'analisi e la ricerca. È considerato un predecessore di Cowrie. Gli honeypot a bassa e media interazione sono spesso degli script Python molto versatili, adatti a quasi tutti i sistemi operativi e non richiedono hardware particolarmente potenti. Gli honeypot ad alta interazione, invece, sono ancora più complessi, perché imitano in modo efficace e completo il sistema che devono proteggere e spesso contengono dati ed informazioni reali affinché l'attaccante pensi di essere entrato davvero nel sistema target. Essi offrono una versione completamente e pienamente funzionate di un servizio, come nel caso di Dockpot, un honeypot che esegue un sistema Linux completo in un'immagine e che espone la connessione SSH, avvalendosi anche di un proxy man-in-the-middle che intercetta tutto il traffico di dati che interessa l'honeypot. Sono così complessi che garantiscono la

separazione delle connessioni e la persistenza, tanto da far pensare ad un attaccante di essere davvero nel sistema target trovando connessioni diverse per ogni IP diverso e vedendo che le modifiche vengono sempre salvate. Sono molto difficili da riconoscere e spesso sono implementati su macchine virtuali isolate dal sistema vero e proprio, anche se sussiste il rischio che un honeypot non perfettamente isolato diventi una porta di accesso per il sistema da difendere, specie se l'attaccante è molto esperto. Questa tipologia di honeypot è detta ad alta interazione perché coinvolge pienamente l'attaccante, come ad esempio HoneyPLC, che simula modelli PLC di diversi vendor, oltre a fornire molte altre funzionalità e log che riesce a raccogliere. Consentono quindi agli attaccanti di interagire con un sistema reale, offrendo moltissime funzioni. Gli honeypot possono essere esposti alla rete, oppure possono essere posizionati strategicamente in una rete interna nei punti in cui è più probabile che un attaccante cerchi di entrare nella rete. Quando si lavora con degli honeypot, è importante tenere presenti alcuni accorgimenti di sicurezza: per esempio, i servizi honeypot non dovrebbero essere eseguiti con privilegi di root, servizi con SSH o FTP dovrebbero essere in esecuzione sulle porte predefinite, disabilitando nel caso di SSH l'autenticazione delle password e il login di root per il vero server SSH e spostando il servizio reale su una porta non standard per proteggerlo. È consigliabile anche prestare attenzione ai rischi legati a possibili errori, creando ad esempio un alias SSH e gestendo con cura i backup sia quando si usano distribuzioni automatiche basate su strumenti come Ansible e Puppet, sia quando ci si affida a provider VPS esterni che sono a rischio di subire attacchi anche pesanti. È utile anche considerare un certo livello di personalizzazione per evitare che gli attaccanti scoprano in fretta di trovarsi in un honeypot, ad esempio modificando certe credenziali predefinite e troppo scontate. Gli honeypot ad alta interazione offrono un livello di personalizzazione più alto, mentre per quelli a bassa e media interazione è più frequente il ricorso a nomi utenti, password e nomi di sistema predefiniti. Ci sono degli accorgimenti da adottare anche per quanto riguarda il monitoraggio dei log, che contengono dati molto preziosi da analizzare e che possono essere inseriti in un sistema centrale, come Elastic o Splunk, che indicizza i dati generati, consente di monitorare tutta l'infrastruttura raccogliendo tutti i dati dei vari honeypot e rende disponibili i dati di log per la dashboard. Si possono distinguere anche altri tipi di honeypot in base a come appaiono queste trappole: vi sono gli email honeypot, i database honeypot, i malware honeypot, gli spider honeypot e gli honeybot. Gli email honeypot, o spam traps, sono degli indirizzi email pensati per attirare email di spam per studiarle e per deviarle da indirizzi email legittimi; questo tipo di honeypot è utilizzato spesso dagli internet service provider per individuare e bloccare degli spammer oppure per aggiornare i servizi di posta elettronica e proteggerli meglio dalle spam. Si crea una indirizzo mail fake nascosto che diventa un facile bersaglio per gli spammer perché solo un address harvester automatizzato riesce a trovare un indirizzo nascosto e quindi si può facilmente individuare la posta spedita a quell'indirizzo come spam, consentendo di bloccare l'IP di chi invia spam e classificando quel tipo di messaggi come spam, riuscendo così a proteggere gli utenti delle caselle mail. I database honeypot sono dei database che non contengono dati sensibili che attraggono i malintenzionati e che servono a studiare l'evoluzione degli attacchi ai database, come SQL injection. I malware honeypot sono delle

copie di software o di API (Application Programming Interfaces) studiati appositamente per attrarre attacchi malware al fine di studiare i malware e migliorare le difese nei loro confronti. Gli spider honeypots sono bot e ad-network crawlers che intrappolano altri bot o crawler malevoli attirandoli in pagine web accessibili solo a crawler automatizzati. Infine gli honeybots sono la tipologia più recente di honeypot, sviluppati nell'ambito della ricerca per interagire con gli hacker e risultare ancora più sofisticati e convincenti. Gli elementi necessari per una strategia di difesa che comprende gli honeypot sono facilmente intuibili da quanto spigato in precedenza. Un honeypot deve apparire come un target molto facile, con delle configurazioni errate o delle password deboli, appetibile per un attaccante in quanto porta di accesso facile a dei dati importanti. Deve essere ovviamente ben isolato per impedire il movimento laterale di un attaccante, deve includere un attento monitoraggio e raccolta dei log per studiare a fondo le mosse dell'attaccante e deve prevedere un sistema di alert per far presente il prima possibile ai responsabili l'affacciarsi di un attacco. I dati raccolti da questi honeypot devono essere ben custoditi per essere analizzati, per individuare nuove strategie di attacco, per studiare come migliorare la difesa e per capire in ambito forense chi sta portando avanti una certa tipologia di attacchi, magari ripetuta. Sia che si tratti di un honeypot che interagisce direttamente con l'attaccante, sia che si tratti di un honeypot invece passivo che si limita a registrare dati di log, è fondamentale tenere impegnati gli attaccanti i più a lungo possibile, evitando che si accorgano di essere finiti in una trappola per raccogliere il maggior numero possibile di dati.

Casi di studio interessanti, applicazioni degli honeypot ed esempi di honeypot.

Gli honeypot sono strumenti molto versatili e potenti ed è interessante riportare qualche caso di studio relativo alla loro applicazione pratica. Nel 2013 grazie agli honeypot gli esperti di sicurezza hanno potuto studiare da vicino e contrastare una campagna botnet basata sul Citadel Malware che colpiva soprattutto le istituzioni finanziarie. L'honeypot riproduceva fedelmente un servizio finanziario vulnerabile ed ha permesso agli esperti di studiare come otteneva informazioni e di capire meglio il funzionamento dei command-and-control server per poter fermare questa botnet e prevenire gli attacchi alle istituzioni finanziarie. È importante ricordare anche il successo di Cowrie, un honeypot basato su SSH e Telnet usato per attrarre attaccanti che compiono attacchi di brute force contro servizi SSH. L'utilizzo diffuso di questo honeypot ha permesso di registrare numerosi tentativi di brute force, dando la possibilità agli esperti di capire il comportamento degli attaccanti, di individuare dei pattern di attacco e delle credenziali utilizzate spesso con successo. Questo ha aumentato la sicurezza, evidenziando delle credenziali non sicure da non utilizzare più ed indicando delle ulteriori misure di sicurezza di hardening dei sistemi. Un caso molto interessante da studiare è quello di Nepenthes honeypot, utilissimo nel bloccare gli attacchi condotti da **script kiddies**. Nepenthes è infatti un honeypot a bassa interazione molto abile nell'attirare e catturare attacchi automatizzati, realizzati da script kiddies che si avvalevano di script già disponibili pubblicamente e non modificati. È un honeypot molto versatile, che non consuma troppe risorse e particolarmente abile nel trovare malware e registrare i loro payload, usato anche per lo studio di botnet o di worm come Conficker worm, Sasser e

Blaster. L'utilizzo di questo strumento ha limitato in modo significativo le attività malevole di hacker non esperti come gli script kiddies, perché catturava facilmente gli attacchi realizzati con script disponibili pubblicamente e gli attaccanti script kiddies, essendo inesperti, non modificavano gli script in modo efficace per aggirare questa trappola. Nepenthes ha ridotto gli attacchi automatizzati e portati avanti da script kiddies, aiutando anche a studiare i metodi di attacco di questi hacker non esperti ma comunque in grado di fare dei danni. Gli honeypot sono uno strumento efficace contro gli script kiddies, proprio perché si basano sulle vulnerabilità non troppo complesse che sono target degli strumenti automatici e degli script pre-compilati che utilizzano questi hacker non esperti e così la loro azione malevola viene deviata e allontanata dai sistemi veri e propri. Sono particolarmente abili nell'intercettare gli scanner e nel riconoscere gli exploit kit usati dagli script kiddies, soprattutto quando il target diventano dei dispositivi IoT che hanno scarse difese e che quindi diventano un bersaglio facile anche per degli hacker inesperti. Non solo Nepenthes, ma anche Cowrie e Dionaea sono stati efficaci nell'intercettare gli script kiddies, i quali non hanno capito di trovarsi in una trappola e sono quindi stati bloccati. Gli honeypot sono utili non solo contro gli script kiddies, ma anche contro hacker esperti, tanto che nel 2009 gli honeypot di The Honeypot Project hanno individuato le prime fasi di un possibile attacco con un malware realizzato da APT1, uno gruppo sponsorizzato dalla Cina. I dati raccolti dagli honeypot hanno permesso di capire le tattiche e gli strumenti utilizzati da questo gruppo e di evitare un attacco su larga scala molto dannoso. Gli honeypot hanno avuto un ruolo importante anche nel contrastare gli attacchi DDoS portati avanti da Mirai Botnet nel 2016: sono stati creati degli honeypot che hanno imitato i dispositivi IoT colpiti e questo ha dato modo ai ricercatori e ai professionisti di capire il funzionamento di questa botnet e della sua diffusione, fermando questi attacchi e capendo come migliorare le difese per future minacce basate su botnet e soprattutto facendo luce sulle vulnerabilità dei dispositivi IoT e sulla necessità di migliorare la loro sicurezza. L'utilizzo degli honeypot aiuta anche a studiare delle patch di sicurezza mirate quando emerge una nuova vulnerabilità sfruttabile, tanto che Windows ha lanciato un progetto chiamato "HoneyMonkey" che si basa su una rete di macchine virtuali con versioni di Windows e di Internet Explorer che cercano siti malevoli che sfruttano delle vulnerabilità dei browser. Sono state trovate migliaia di siti in grado di sfruttare vulnerabilità ancora non corrette e potenzialmente in grado di scatenare attacchi di tipo zero-day e questo ha aiutato a creare delle patch di sicurezza per vulnerabilità non ancora sfruttate, prevenendo un gran numero di attacchi. Tutti questi esempi pratici aiutano a comprendere la versatilità degli honeypot, efficaci nel contrastare minacce complesse come la Mirai Botnet ed utili per limitare gli script kiddies, per studiare vulnerabilità esistenti e per agire contro vulnerabilità non ancora pienamente sfruttate. È già stata spiegata l'importanza degli honeypot in termini di ricerca e di threat intelligence e per questo è stato creato the Honeypot Project, una rete globale di honeypot utilizzata per raccogliere informazioni e dati sui vari tipi di attacchi informatici. Si tratta di un'organizzazione di ricerca no profit e volontaria che utilizza gli honeypot per studiare le minacce in termini di sicurezza e migliorare le tecniche di difesa. Gli honeypot possono avere delle applicazioni molto concrete, dato che sono stati utilizzati anche dalle istituzioni per individuare ed arrestare

criminali informatici. Per esempio, l'operazione OTF Greenlight/Trojan Shield, condotta dall'FBI con la polizia olandese e danese e con la collaborazione della US Drug Enforcement Administration e dell'Europol ha usato un principio simile a quello degli honeypot. È stata creata dall'FBI e dalla polizia australiana una compagnia chiamata ANOM che offriva canali di comunicazione criptati e dispositivi per comunicazioni sicure e criptate nell'attesa che fossero utilizzati dai criminali, attirandoli con la promessa di avere comunicazioni sicure e non tracciabili per i loro affari sporchi. Ben 12000 dispostivi sono stati utilizzati da criminali e malavitosi in più di 100 paesi e questa operazione ha portato all'arresto di ben 800 criminali e al sequestro di 8 tonnellate di cocaina, 2 tonnellate di metanfetamine e molto altro ancora.

Per citare qualche altro esempio di honeypot, si può pensare ad honeyd, un honeypot a bassa interazione con un software open source in grado di creare diversi host virtuali con cui riprodurre diversi servizi di rete. Questo software è molto diffuso, anche se non molto aggiornato, e permette un buon livello di personalizzazione. Anche Dionaea è un honeypot a bassa interazione in grado di simulare servizi vulnerabili come FTP o HTTP per catturare malware ed interagisce molto bene con Nepenthes. È veramente utile per la malware analysis e viene spesso utilizzato anche nelle reti di honeypot. Altri honeypot interessanti sono T-Pot, un honeypot ad alta interazione che unisce le funzioni di vari honeypot già analizzati in precedenza, NetBait, specializzato nello studio delle minacce sulla rete come gli attacchi DDoS e ConPot, che imita sistemi di controllo industriali vulnerabili, supportando la sicurezza di infrastrutture critiche come impianti energetici o industriali. HoneyC è un software in grado di simulare un client che si collega ad un server e sa riconoscere se si tratta di un server pericoloso o malevolo e crea quindi degli honeypot a bassa interazione. PhoneyC emula vari browser per riconoscere contenuti dannosi nelle pagine web, per esempio degli script malevoli inseriti in una pagina web apparentemente innocua ed anche mapWOC è un software open source che viene eseguito su una macchina virtuale per analizzare il traffico dati. Se si parla di honeypot ad alta interazione, bisogna citare Sebek, un sistema ad alta interazione che raccoglie dati sulle attività degli attaccanti e le invia ad un server per l'analisi e la memorizzazione, e Argos, che imita interi sistemi hardware e sa identificare immediatamente del traffico malevolo per controllarlo e raccogliere dati. La ricerca per la creazione di honeypot sempre più credibili e verosimili è molto attiva; per esempio, nel 2023 è stata lanciata HASH (http Agnostic Software Honeypot), un framework open source per creare e lanciare honeypot a bassa interazione sempre più flessibili.

Aspetti positivi e negativi degli honeypot.

Gli honeypot sono molto utili per proteggere i sistemi, attirando su di sé l'attenzione degli hacker e fornendo loro informazioni non importanti. Inoltre aiutano a migliorare lo studio nell'ambito della threat intelligence, grazie alla comprensione delle tendenze in termini di attacchi. Per esempio, la famiglia di bot Chalubo è stata scoperta dai SophosLabs grazie ad un attacco avvenuto contro un loro honeypot nel settembre 2018. Chalubo botnet aiuta la diffusione di malware come Xor.DDoS oppure Mirai ed è stata studiata a fondo dai ricercatori di SophosLabs, che hanno compreso il funzionamento di questi bot, basati su un downloader, su un Lua command script e su un main bot ottimizzato per hardware con un processore

Intel su macchine con architettura x86. I ricercatori hanno anche capito che questi bot portano avanti attacchi brute force per il login su server SSH e tutte queste preziose informazioni sono state raccolte proprio grazie agli honeypot, che servono per monitorare le minacce che circolano e quelle emergenti al fine di studiare strategie difensive utili. Tra i vantaggi degli honeypot va ricordato il numero bassissimo di falsi postivi, dato che interagiscono con gli attaccanti ed inviano dati solo quando un attacco è effettivamente in corso e sono vantaggiosi in termini di costi economici, anche perché non richiedono particolari risorse hardware. A differenza degli IDS che generano molti falsi positivi, gli honeypot non danno falsi positivi, anche perché un utente legittimo non ha motivo di interagire con questi strumenti. Essi aiutano a prevenire altri attacchi informatici, sia perché tengono impegnati gli attaccanti distraendoli da altri obiettivi, sia perché aiutano a trovare dei pattern e delle metodologie di attacco che vengono studiate in tempo reale. Possono anche aiutare a notare attività sospette alla base magari di un attacco zero-day, prevenendo gli ingenti danni generati da questa tipologia di attacchi. Danno un contributo importante anche per l'analisi forense in caso di attacco, perché aiutano a ricostruire un attacco, a capire l'entità dei danni e supportano le attività di ricostruzione, ripresa ed analisi a seguito di un attacco. Oltre alla prevenzione e allo studio degli attacchi, gli honeypot portano ad un Decreased Mean Time to Detect (MTTD), il che significa che riducono notevolmente il tempo necessario per scoprire che un attacco è in corso, dando la possibilità a chi si occupa della sicurezza di intervenire più rapidamente ed efficacemente a difesa dei sistemi. Se un attaccante viene fermato grazie agli honeypot, si riduce notevolmente anche il tempo passato dall'attaccante nel sistema, riducendo i tentativi dell'attaccante per trovare password, username, tentare privilege escalation e quant'altro. Gli honeypot sono utilizzati da aziende come Google, che li usano nell'ambito della threat intelligence per studiare i vari tipi di attacchi e di minacce per poi personalizzare le difese per i sistemi Google, ed anche JPMorgan fa uso di honeypot per studiare gli hacker e raccogliere informazioni riguardo alle loro attività, comportamenti e metodologie. A differenza dei firewall che proteggono solo da minacce esterne, un honeypot può difendere anche da violazioni interne, portate avanti ad esempio da un dipendente infedele, se piazzato nella rete interna. Nonostante queste funzioni molto utili, gli honeypot presentano degli aspetti negativi di cui tenere conto. Innanzitutto, non offrono una difesa attiva o una forma di prevenzione, perché raccolgono dati solo in caso di attacco vero e proprio e questo attacco deve colpire direttamente l'honeypot. Questi sistemi devono essere costantemente aggiornati, devono essere perfettamente isolati per non diventare la porta di accesso dei malintenzionati a tutto il sistema e devono avere un certo livello di complessità per non essere subito riconosciuti dagli hacker come honeypot, i quali potrebbero tentare attività di fingerprinting per accertarsi di avere a che fare con una trappola o per provare a carpire informazioni sulla rete a cui accedere. Sarebbe pericoloso che un hacker si accorgesse di avere a che fare con un honeypot, anche perché potrebbe tentare di ingannare a sua volta i gestori del sistema. Per questo motivo, potrebbe essere utile pensare ad un honeywall, che evita che da un honeypot possa partire un attacco verso la rete da proteggere. Gli honeypot devono essere configurati in modo appropriato, per evitare che un attaccante esperto possa trovare delle

vulnerabilità da sfruttare. Bisogna sempre ricordare che varie tipologie di attacco avvengono senza essere rintracciate dagli honeypot, per cui non bisogna mai abbassare la guardia e vanno tenute presenti le limitazioni legali che possono essere presenti in alcuni Paesi, come l'Italia, all'uso degli honeypot. L'uso di honeypot può sollevare delle problematiche legali ed etiche, legate per esempio alla raccolta di dati, alla conseguente violazione della privacy e alla mancanza di un esplicito consenso da parte dei proprietari dei dati. È inoltre in dubbio dal punto di vista etico e legale la correttezza di usare degli strumenti per trarre in inganno gli attaccanti, anche se questo ha lo scopo di migliorare la sicurezza. Ci si può chiedere se questi strumenti vadano ad incitare attività illegali, stimolando degli attaccanti a provare un exploit. Un'altra problematica è collegata all'utilizzo di questi strumenti per carpire i dati di cittadini normali e non criminali informatici da fermare, quando ad esempio vengono creati dei siti trappola per capire chi si avvale di un servizio craccato o piratato. Gli honeypot sono veramente problematici per il diritto dell'Unione europea: per esempio, la direttiva 95/46/EC, chiamata EU Data Protection Directive del 1995, ora sostituita dal regolamento n. 216/679 o GDPR (general data protection regulation) afferma che i dati devono essere forniti con un esplicito consenso (art.7 lettera A) e devono essere utilizzati con uno scopo preciso per adempiere ad un obbligo del soggetto che ottiene i dati (lettera C). I dati raccolti tramite honeypot non vengono forniti con il consenso esplicito, libero ed informato da parte dei criminali informatici, ovviamente, ma questo non è l'unico aspetto problematico. Sulla base della Data Protection Directive, i dati raccolti dagli honeypot, compresi gli indirizzi IP, sono classificati come dati personali ai sensi dell'articolo 2a, come confermato anche dalla Corte di giustizia dell'Unione europea nel caso Scarlet Extended SA vs. Socit belge des auteurs compositeurs et diteurs. Dall'indirizzo IP si può risalire ai dispositivi e all'identità di una persona ed anche gli IP dinamici sono da considerarsi dati personali perché un internet service provider potrebbe comunque risalire al dispositivo e alla persona collegata a quell'indirizzo IP. I dati personali sono protetti dalla privacy e quindi raccogliere questi dati con gli honeypot senza un consenso esplicito ed informato rappresenta una violazione della privacy. L'utilizzo di honeypot potrebbe creare problemi legali di responsabilità qualora un honeypot avesse delle vulnerabilità e venisse controllato da un utente malintenzionato per attaccare ad esempio un'altra azienda, la quale potrebbe rifarsi su chi avrebbe dovuto mantenere l'honeypot sicuro ma non ci è riuscito. Vi sono anche problemi di giurisdizione, come tutte le questioni legate al digitale. Menzionare alcuni provvedimenti legali direttamente riconducibili agli honeypot aiuta a comprendere come la questione sia complessa e controversa dal punto di vista legale. Il Wiretap Act statunitense afferma che le comunicazioni elettroniche non possono essere intercettate e quindi il traffico intercettato dagli honeypot potrebbe risultare problematico proprio per la mancanza di consenso da parte degli attaccanti coinvolti. Gli honeypot potrebbero essere giustificati solo se si tratta di comunicazioni interne di un'azienda e che non coinvolgono terze parti ai sensi dello Stored Communications Act. Il Computer Misuse Act del Regno Unito punisce gli accessi non autorizzati ai sistemi informatici e gli honeypot si trovano in una zona grigia perché sono legali purché non vadano a fomentare l'accesso non autorizzato ad un sistema. Questi sistemi sono fatti appositamente per attirare degli hacker e per questo potrebbero avere

problemi ai sensi della legge. Sorgono problemi legali anche quando vengono raccolti dati di utenti non criminali, magari anche accidentalmente, quando ad esempio un honeypot sviluppato in ambito accademico per la ricerca va a raccogliere dati di studenti innocenti. Anche la legge italiana non autorizza pienamene l'utilizzo di tecnologie come gli honeypot, il cui utilizzo potrebbe configurare un reato informatico.

Altre deception technologies e sviluppi futuri.

Gli honeypot rientrano nel settore della deception technology, che diventerà sempre più sofisticata anche grazie all'apporto dell'intelligenza artificiale e del machine learning, in grado di aiutare a creare strumenti sempre più raffinati per la difesa e la cybersecurity e questi strumenti possono essere facilmente combinati tra loro. Si potrebbe fare ricorso non solo a singoli honeypot, ma anche ad una rete di honeypot, chiamata honeynet, che simula una rete vera e propria per distogliere l'attenzione degli attaccanti da una vera rete. Una honeynet è una rete con vari dispositivi creata apposta per essere attaccata e per studiare il comportamento degli attaccanti su una rete e prevede un honeynet management system, che monitora e controlla l'ambiente honeynet, una rete di honeypot o altri dispositivi con varie funzioni e un production system isolato dall'honeynet. Questa soluzione è adatta per proteggere grandi reti ed aiuta a raccogliere una significativa quantità di informazioni sugli attaccanti e sulle metodologie di attacco alle reti, imitando in modo efficace una rete vera e propria gestita di solito da uno o più server. Esistono anche gli honeytokens, che sono delle risorse, dei dati o delle credenziali fake che lanciano un alert quando un malintenzionato cerca di accedervi, rappresentando un'alterativa più facile ed immediata all'utilizzo di veri e propri honeypot. Questi dati possono essere integrati anche nei sistemi esistenti senza dover simulare completamente un servizio, una web app o un software e sono molto facili da monitorare e controllare. Sarà interessante valutare il ruolo dell'intelligenza artificiale, che consentirà una gestione più veloce e più efficiente della grande quantità di dati raccolti e che porterà ad un'analisi più sofisticata e ad un'individuazione più veloce di pattern ed altre minacce, anche emergenti o di tipo zero-day.