Cyber Deception Technology, nuova frontiera nell'arte della guerra

Il concetto è semplice: l'espressione **"inganno militare"** si riferisce alla possibilità di ingannare i nemici durante una guerra o una rappresaglia. Ciò si ottiene normalmente alterando i fenomeni di contorno come **le informazioni, la comunicazione e la percezione psicologica** ad uso di un più ampio scopo strategico.

Kevin Mitnick (nome in codice "condor", famoso hacker americano ispiratore di tantissimi film sull'hacking, oltre ad essere stato l'inventore dello *"spoofing ip"*), nel suo libro ***The Art of Deception*** riportava:

«La mente umana è un'invenzione meravigliosa. È interessante notare quanto riesca a essere creativa la gente quando si tratta di inventare modi subdoli per ottenere quanto le pare o per togliersi da una situazione spinosa. Dovete usare la medesima creatività e immaginazione per proteggere i sistemi informatici e di informazione nei settori pubblici e privati. Perciò, gente, quando pensate alle politiche di sicurezza delle vostre aziende… siate creativi e pensate fuori dal sentiero tracciato».

La cyberwar è del tutto simile alle guerre reali, ne abbiamo già parlato nell'articolo Stati e Guerre senza confini geografici pubblicato su *Safety & Security Magazine*; ma ad oggi come possiamo sfruttare "l'arte dell'inganno" nella cybersecurity per aumentare la sicurezza delle infrastrutture informatiche, proprio come Kevin Mitnick ci incitava a fare?

Come sappiamo, il concetto di *honeypot* è presente da tempo, ma si tratta di un ***ecosistema bersaglio auto-consistente*** che funge da "trappola" per eventuali intrusioni informatiche.

Lo step successivo è quello di ***creare delle trappole in-line*** alle applicazioni, che risultino esposte come ***parte integrante dell'applicazione stessa***, in maniera customizzabile e gestibile, che portino l'attaccante in una bolla creata ad arte per simulare vulnerabilità finalizzate a depistarlo dal bersaglio reale, anche esponendo ***dati simili*** a quelli dall'applicazione da proteggere.

Ad esempio, un utilizzo della cyber-deception sulle web-application, può essere implementata simulando la presenza di url (esposte sullo stesso dominio che si vuole proteggere, magari come pagine di backup o altro), affette da note vulnerabilità come ad esempio ***sql-injection, XSS o Remote Code Execution*** che consentono di ingannare i potenziali aggressori e condurli su percorsi di attacco creati per loro, monitorandone gli avanzamenti attraverso il ***Security Operation Center*** pronto ad agire una volta raccolte tutte le tracce essenziali per poter impugnare un'analisi forense.

Tali applicazioni "parallele", di fatto, non saranno altro che delle ***honeypot "multi layer"*** esposte in "bolle" completamente separate dalle reti aziendali (ad es. utilizzando hypervisor o virtualizzatori vari) che conterranno vulnerabilità note in modalità "inline" alle applicazioni da proteggere, magari riutilizzando e customizzando applicazioni già presenti negli hub-container pubblici per la creazione di sandbox.

Ovviamente **la customizzazione risulterà fondamentale,** in particolar modo per rendere le pagine simili al portale da proteggere e, quindi, non far accorgere i potenziali aggressori ***di essere atterrati su qualcosa di noto***, magari da loro utilizzato per precedenti esercitazioni di attacco.

A questo punto il criminale informatico, qualora sia riuscito

a completare l’attacco sul sito “fake”, potrebbe:

1. ritirarsi e immagazzinare i dati “fake” pensando che questi siano corretti;
2. in caso di attivismo, pubblicare i dati su repository pubblici (ad es. pastebin), oppure effettuare deface del sito “fake”, ovviamente non l’applicazione principale (il dominio da proteggere);
3. incorrere in potenziali azioni legali, dovute alle tracce lasciate sui sistemi e acquisite dal Security Operation Center di competenza.

Nel secondo caso occorre prestare attenzione, in quanto potrebbero esserci implicazioni sul ***brand e nella web reputation dell’impresa:*** l’inganno non deve influenzare gli scenari del mondo reale.

Come difendere *brand & web reputation* dopo una *deception*

In un contesto così labile tra difensore e attaccante, che pubblica in rete informazioni “fake” provenienti da un nostro sito, ***rispetto all’opinione pubblica, come occorre comportarci?***

Sicuramente l’aspetto più importante sta nel rendere inviolabile il “miele” contenuto all’interno delle applicazioni da proteggere e, su questo fronte, tutte le tecniche di guerra risultano lecite.

Applicando tutto questo, occorrerà attraverso la **comunicazione** (che vedevamo all’inizio essere uno **tra i principali attori nell’arte dell’inganno**), proteggere il brand da eventuali attacchi sulle fonti pubbliche. Questo forse in molte aziende potrebbe essere oggi ancora difficile da sostenere, per una mancanza di specifiche competenze o reattività nell”attraversamento dei processi aziendali di Cyber Security.

Conclusioni

L’arte della *deception* è stata avviata nel lontano 1999 con le *honeypot* che hanno trainato il mercato di quel periodo. Dopo molto entusiasmo si è avuto negli anni successivi un forte arresto, tanto che si parlò di ***“inganno dell’inganno”*** che si concluse nel 2014 quando tali concetti cominciano a riprendere forma, anche se in modo differente.

Probabilmente questa sarà una nuova branca di sviluppo nella cybersecurity nel prossimo futuro. Gartner, all’inizio del 2019, parla di ***“Cyber Deception Technology”*** (o CDT) e stima che nel 2019 solamente il 10% delle aziende introdurrà strumenti o poc – e, soprattutto, sarà organizzato per gestire una corretta comunicazione – su questo nuovo fronte. Un problema è legato anche a una carenza di listino di questo genere di strumenti, che risultano oggi limitati se non completamente assenti.

Nelle guerre, come sappiamo, ***non esistono limiti nella sperimentazione tecnologica:*** ce lo insegna Mitnick ma anche gli eventi e anche questa branca di “guerra cibernetica” non è da meno. Il tempo ci farà comprendere ***se questa nuova visione dell’inganno*** consentirà di fornire supporto alle grandi aziende oppure se si tratti, come in molti casi, di architetture inutili acquistate e poi non più utilizzate, collezionate in *rack* spenti nei datacenter.

Articolo a cura di **Massimiliano Brolli**

https://www.ictsecuritymagazine.com/articoli/cyber-deception-technology-nuova-frontiera-nellarte-della-guerra/