Deception Techniques for Every Stage of A Cyber Attack

CounterCraft

The goal of cyber deception is to detect attacks on an organization's network, either before they happen or in the midst of the attack. Deception can confuse and misdirect the attacker as well as help to understand what assets have been compromised.

When you break down a cyber attack, you find patterns and actions that are commonplace. Every cyber attack consists of various stages, from pre-breach to the moment of impact. With deception, every stage is an opportunity to trip up and trap cyber criminals. The more you understand the different steps a cyber criminal takes, the more opportunities you have to stop them.

Keep reading to get a breakdown of the stages of a typical cybersecurity incident. Find out what the different stages are called, as well as an example of what threat actors could be doing in each stage. Deception technology can halt threat actors at every stage, even pre-breach and during lateral movement. Deception can help you fight cyber attacks, every step of the way.

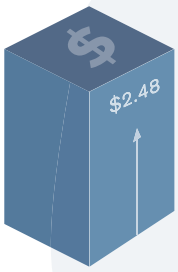
There are 14 stages in the MITRE ATT&CK matrix

Deception has an answer for just about all of them

Deception Allows You To

CUSTOMIZE THE SOLUTION

tailoring it to your organization and your crown jewels.



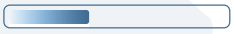
The Deception Technology market is forecast to reach

$2.48

Billion by 2025

Deception Techniques for Every Stage of A Cyber Attack

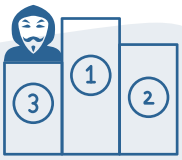
1. Reconnaissance
2. Resource Development
3. Initial Access
4. Execution
5. Persistence
6. Privilege Escalation
7. Defense Evasion
8. Credential Access
9. Discovery
10. Lateral Movement
11. Collection
12. Command and Control
13. Exfiltration
14. Impact



Publicly disclosed cybersecurity incidents increased by

22%

in the second half of 2020.



If cybercrime were a country with a GDP, it would be the world's third-largest economy after the U.S. and China.

BREACH TACTICS IN 2021

75% of breaches featured hacking

32% included phishing or social engineering

28% involved malware

Recon Phase / They're trying to get in

1 Reconnaissance

The adversary gathers information, such as contacts and vulnerabilities, to plan their attack.
What the attacker is doing: Researches Business X on LinkedIn, corporate webserver and anywhere else he can think of.
How deception works to stop them: Deploy external campaigns to find out when someone is looking for information on your organization.

2 Resource Development

The attacker collects tools to try to exploit and breach the discovered attack surface, and/or works on creating a phishing template to trick employees.
What the attacker is doing: Combs the deep web for access information, such as a compromised machine in the form of a bot or compromised credentials, vulnerabilities, and any other relevant information. Doesn't find anything useful for direct access, but creates a legitimate looking email template to be used against employees.
How deception works to stop them: Place external breadcrumbs to get threat actors to enter a deception buffer zone, where they will leave clues about what they are after.

Attack & Expand Phase / They gain access to the network

3 Initial Access

The threat actor gains an initial foothold in the network.
What the attacker is doing: Sends an email to 20 people in Business X and waits for someone to click. Endpoint compromised and access granted!
How deception works to stop them: Protect user networks by adding deception network assets that will be completely unexpected by the adversary. Or, deploy counter-phishing deception campaigns to deflect attackers into deception networks. When the attacker accesses them, a highly trustworthy alert is sent to the security team.

4 Execution

The adversary runs malicious code somewhere in the system.
What the attacker is doing: The attacker runs malicious code and the user unknowingly executes malware on the endpoint.
How deception works to stop them: Any endpoints that are part of the deception network will give you a clear alert when new code is run or there are inserts in other processes. The the attacker has landed in a minefield, full of breadcrumbs in memory, files, and shared resources to access, and they don't even know it.

5 Persistence

The attacker works to maintain their foothold in the system.
What the attacker is doing: The malware gains persistence in the system by making sure that the software component will run in each machine restart or in a periodic task, or whenever a legitimate user application is loaded.

6 Privilege Escalation

The threat actor works to gain higher privilege permissions on the network.
What the attacker is doing: Enumerates several techniques, for privilege escalation, and gains privileges using a dll hijack technique.
How deception works to stop them: Place breadcrumbs, such as false backup or configuration files, across the hosts, or implant credentials in workstations memory, designed to tempt the threat actor to access this goldmine of information, that could contain account credentials with higher privileges. If the attacker tries to use the decoy information, an alert will trigger.

Defense Evasion

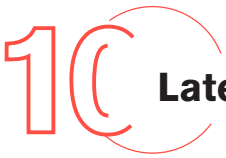
The adversary works to avoid detection, encrypting connections and data, and disabling security software.
What the attacker is doing: Malware uses several emulation and virtualization detection techniques and waits for human behavior in the machine in order to detonate.
How deception works to stop them: Place breadcrumbs that look like security software but will send an alert if it is disabled or uninstalled.

Credential Access

The attacker looks for credentials they can steal.
What the attacker is doing: Dumps credentials from memory
How deception works to stop them: Have breadcrumbs in place with fake credentials, strategically named and placed to be very tempting to threat actors.

Discovery

The threat actor is trying to learn all they can about a network.
What the attacker is doing: Looks for local information about the network on the computer and finds the running processes, general services and software, and also the information that the computer configuration and files could provide about where the access was obtained.
How deception works to stop them: Create active false documents about network topology and access privileges, which, when opened can:
– Send an alert to your security team
– Take the threat actor to a deception environment
– Provide false information
Add assets that the attacker can't distinguish from real assets, forcing the attacker to play 'minesweeper'.



Lateral Movement

The attacker does everything they can to gain access to other machines.
What the attacker is doing: Exploits a zerologon vulnerability against the primary domain controller.
How deception works to stop them: Offer a number of easily discoverable assets, like domain controllers, that lead to deception environments only.

Collection

The adversary collects the data they came for, the data they need to achieve their goal.
What the attacker is doing: Obtains classified information about sensitive users,
How deception works to stop them: Plant false information mimicking the real information an adversary could be looking for. Get alerts when the files are opened. Include further links in those files to act as beacons, when the links are followed through to other deception networks, diverting the attacker from the internal network to an external deception campaign.

Damage Phase / They are getting what they want and compromising the system

12 Command and Control

The attacker is communicating with the compromised system, usually in a way that appears to be normal, expected traffic to remain hidden.
What the attacker is doing: Connects with the C&C using DNS tunneling
How deception works to stop them: If the attacker enters the deception environment, it will be much easier to detect any covert communication mechanism and use that to flag other incidences of this covert system in other network areas.

13 Exfiltration

This is the stage in which the attacker takes the data that they came for.
What the attacker is doing: Encrypts the data so security systems do not detect the exfiltration and sends it back to the attacker C&C system.
How deception works to stop them: Deception has provided the intruder with fake information, backed up with breadcrumbs that lead to it, making the attacker think they've got what they came for. Even if links baked into this information are accessed from outside the enterprise, the security teams get an alert, in real time.

14 Impact

At this time, the adversary manipulates or destroys data, sometimes covertly in order to maintain a presence on a network.
What the attacker is doing: Encrypts first system to then charge a ransom. Then moves on to encrypting all systems. May exfiltrate sensitive information.
How deception works to stop them: Detect the attacker in an early phase of the attack. Detects encryption of information in the deception hosts, gathers data on modus operandi to protect other networks. Provides the threat actor with false information to exfiltrate, limiting impact.

About CounterCraft

CounterCraft is the next generation of threat intelligence. The CounterCraft Cyber Deception Platform offers active defense powered by high-interaction deception technology. Countercraft detects threats early, collects personalized, actionable intelligence, and enables organizations to defend their valuable data in real time.

CounterCraft is recognized worldwide for its groundbreaking contribution to the deception technology market and operates in more than 20 Fortune500 Index companies globally, including financial institutions, governments and Law Enforcement Agencies. Founded in 2015, CounterCraft is present in New York, London, and Madrid, with R&D in San Sebastián (Spain). Learn more at **www.countercraftsec.com**.

Download our latest documents at

countercraftsec.com

or if you prefer contact us at

craft@countercraftsec.com