

Watering Hole Attacks - SY0-701 - 2.2

Definition: A targeted attack where a threat actor compromises a website that is frequently visited by a specific group of users they want to target.

The Analogy: In nature, a predator doesn't chase its prey; it waits near a watering hole where victims are known to gather. Similarly, the attacker "poisons" a digital location where their intended victims congregate.

How a Watering Hole Attack Works

1. **Identify the Target Group:** The attacker chooses a group they want to infiltrate (e.g., employees of a specific defense contractor, members of a particular industry).
2. **Research and Compromise:**
 - The attacker researches which websites this group commonly uses (e.g., industry forums, news sites, software download portals).
 - They find a vulnerability in one of these third-party websites and compromise it.
3. **Infect the Website:**
 - The attacker adds malicious code to the compromised website. This code is often designed to be stealthy and may only activate for visitors from specific IP ranges (the target organization).
4. **Wait for Victims:**
 - When a user from the target group visits the compromised site, the malicious code automatically attempts to exploit a vulnerability in their browser or plugins to install malware.
5. **Gain Access:**
 - If successful, the malware gives the attacker a foothold inside the target organization's network.

Key Characteristics

- Targeted: The attack is not broad; it's aimed at a very specific demographic.
- Uses Trusted Sites: The victim is compromised by visiting a legitimate, normally trusted website that has been secretly poisoned.
- Difficult to Detect: Since the user is just browsing a site they trust, they have no reason to be suspicious.

Video Example

- An attacker wants to target Company A.
 - Through research, they discover that employees of Company A frequently visit `www.industry-news-updates.com` to get the latest information.
 - The attacker finds and exploits a vulnerability in `www.industry-news-updates.com` and inserts malicious JavaScript.
 - An employee from Company A visits the site. The malicious code runs, exploits a zero-day vulnerability in the employee's browser, and silently installs malware.
 - The attacker now has access to Company A's network, all because an employee visited a trusted industry website.
-

Summary

- A watering hole attack compromises a trusted, third-party website that a specific group of users visits.
- The goal is to infect members of the target group when they browse to the poisoned site.
- It is a passive and targeted attack, making it very effective and difficult to defend against.