Attack Scenario

Vathna.lay@cadt.edu.kh

Attack Scenario: Water hole

Acme Corporation, a leading tech company, has been targeted by a sophisticated cybercriminal group. The attackers have carefully researched the company's employees and their online habits. They've noticed that many employees frequent a popular local coffee shop, "The Daily Grind." The attackers decide to exploit this pattern.

- The criminals install a malicious device on the coffee shop's Wi-Fi network. This device captures the network traffic of anyone connected, including Acme employees.
- They then set up a fake website that looks nearly identical to the coffee shop's website. This website is designed to exploit a known vulnerability in a popular web browser.
- The criminals send out phishing emails disguised as promotional messages from the coffee shop, urging customers to visit the fake website to claim a discount.
- Unsuspecting Acme employees, using the coffee shop's Wi-Fi, visit the fake website. The exploit in the fake site delivers malware to their devices, giving the attackers a foothold inside Acme's network.
- Now inside the company's network, the attackers can move laterally, stealing sensitive data, installing ransomware, or disrupting critical operations.

Group 1: Understand the attack

- How does a waterhole attack work?
- What makes a location a suitable "watering hole"?
- How do attackers exploit vulnerabilities in the watering hole?

Group 2: Real-World Examples

- **Research and present a real-life case of a waterhole attack**
  - How did it unfold?
  - What were the consequences?
- **Identify other potential "watering holes" that could be targeted**
  - Consider different types of locations, both online and offline.

Group 3: Mitigation and Prevention

- How can individuals protect themselves from waterhole attacks?
- What security measures can organizations implement to defend against such attacks?

Group 4: Critical Thinking

- Why are waterhole attacks effective?
- What are the ethical implications of waterhole attacks?
- What future trends can be anticipated in waterhole attacks?

Attack Scenario: The Malicious USB Drop

The target is a large financial firm with strict security measures in place. The attackers, knowing they cannot easily infiltrate the network directly, devise a plan to exploit human curiosity and trust.

- The attackers create several USB drives that look like they belong to the company, with the logo and even employee names printed on them. These drives are loaded with malware designed to bypass security software and establish a backdoor into the network.
- The attackers strategically "drop" these USB drives in places where employees are likely to find them, such as the parking lot, break room, or near the office building's entrance.
- An employee, intrigued by the found USB drive, plugs it into their work computer, hoping to find out who it belongs to or what's on it.
- The malware automatically executes, silently installing itself on the computer and establishing a connection to the attackers' command-and-control server.
- The attackers now have access to the company's internal network and can start stealing sensitive financial data, customer information, or intellectual property.

Group 5: Understand the attack

- How does a malicious USB drop attack work?
- What makes this type of attack effective?
- What are the different ways malware can be delivered through a USB drive?

Group 6: Real-World Examples

- **Research and present real-life cases of malicious USB drop attacks**
  - ow were they executed?
  - What were the consequences?
- **Find examples of companies that have been targeted with this technique.**
  - What industries are most vulnerable, and why?

Group 7: Mitigation and Prevention

- How can individuals protect themselves from malicious USB drop attacks?
- What security measures can organizations implement to prevent such attacks?

Group 8: Critical Thinking

- Why do people fall victim to baiting attacks?
- How has the threat of malicious USB drops evolved over time?
- What are the ethical implications of this type of attack?


?
Q&A