Cyber Security

2024

Hacker Type

Vathna.lay@cadt.edu.kh

Hacker types

- Group 1: Black hat
- Group 2: White hat
- Group 3: Gray hat
- Group 4: Green hat
- Group 5: Blue hat
- Group 6: State-sponsored hacker
- Group 7: Hacktivist

Research & Profile

- Gather information about your chosen hacker type from credible sources.
- Create a detailed profile including:
  - Motivations: What drives this type of hacker? Financial gain, ideology, curiosity, etc.?
  - Skills & Techniques: What methods and tools do they typically use?
  - Targets: Who or what do they usually attack? Individuals, businesses, governments?
  - Impact: What are the potential consequences of their actions?
  - Real-world Examples: Research and briefly describe at least two real-world incidents involving this type of hacker.

Cybersecurity Implications:

- Analyze the specific threats posed by your chosen hacker type.
- Discuss the vulnerabilities they exploit and the potential damage they can cause.
- Propose cybersecurity strategies and measures to mitigate these risks.

Presentation

- Presentation: should be in english
- Present your findings in a clear and concise format.
- Include visuals (e.g., diagrams, charts) to enhance your explanation.
- Be prepared to answer questions and engage in discussions about your chosen hacker type.

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