**Atividade Proposta: Análise de Dois Ataques Cibernéticos**

**1. Ataque ao Health Service Executive (HSE) da Irlanda**

**1. Data do ataque:** 14 de maio de 2021​[Wikipédia, a enciclopédia livre](https://pt.wikipedia.org/wiki/Ataque_de_ransomware_ao_Health_Service_Executive?utm_source=chatgpt.com)

**2. Tipo de ataque:** Ransomware (Conti)​[Wikipédia, a enciclopédia livre+1Wikipedia, la enciclopedia libre+1](https://pt.wikipedia.org/wiki/Ataque_de_ransomware_ao_Health_Service_Executive?utm_source=chatgpt.com)

**3. Descrição do ataque:** O HSE, sistema de saúde pública da Irlanda, sofreu um ataque de ransomware que resultou na paralisação de todos os seus sistemas de TI. Os invasores utilizaram o ransomware Conti para criptografar dados e exigiram um resgate para a liberação das informações.​[Wikipédia, a enciclopédia livre](https://pt.wikipedia.org/wiki/Ataque_de_ransomware_ao_Health_Service_Executive?utm_source=chatgpt.com)

**4. Vulnerabilidade explorada:** O ataque começou com o envio de um e-mail malicioso contendo um arquivo do Microsoft Excel, que, ao ser aberto, permitiu o acesso dos invasores aos sistemas do HSE. Embora não tenha sido atribuído um código CVE específico, o ataque explorou falhas na segurança de e-mails e na detecção de ameaças.​[Wikipédia, a enciclopédia livre](https://pt.wikipedia.org/wiki/Ataque_de_ransomware_ao_Health_Service_Executive?utm_source=chatgpt.com)

**5. Impactos e/ou prejuízo:** O ataque causou a interrupção de serviços de saúde em todo o país, afetando consultas, exames e procedimentos médicos. Estima-se que o custo para restaurar os sistemas e mitigar os danos ultrapassou dezenas de milhões de euros.​[Wikipédia, a enciclopédia livre+1ElHuffPost+1](https://pt.wikipedia.org/wiki/Ataque_de_ransomware_ao_Health_Service_Executive?utm_source=chatgpt.com)

**6. Tipo de proteção que poderia ter sido aplicada:** Implementação de filtros avançados de e-mail para detectar anexos maliciosos, uso de software antivírus atualizado, treinamento de funcionários para reconhecimento de e-mails suspeitos e adoção de autenticação multifator para acesso aos sistemas.​[Wikipédia, a enciclopédia livre](https://pt.wikipedia.org/wiki/Ataque_de_ransomware_ao_Health_Service_Executive?utm_source=chatgpt.com)

**2. Operação Triangulação – Ataque a Dispositivos iOS**

**1. Data do ataque:** Descoberto em junho de 2023​

**2. Tipo de ataque:** Spyware avançado (exploração de vulnerabilidades zero-day)​[Wikipédia, a enciclopédia livre](https://pt.wikipedia.org/wiki/Opera%C3%A7%C3%A3o_Triangula%C3%A7%C3%A3o?utm_source=chatgpt.com)

**3. Descrição do ataque:** A Operação Triangulação foi uma campanha de espionagem cibernética direcionada a dispositivos iOS. Os atacantes enviavam mensagens iMessage contendo código malicioso que, ao ser processado pelo dispositivo, explorava vulnerabilidades desconhecidas para instalar um spyware. Este spyware permitia o acesso a mensagens, senhas, gravações de áudio e localização do usuário.​[Wikipédia, a enciclopédia livre](https://pt.wikipedia.org/wiki/Opera%C3%A7%C3%A3o_Triangula%C3%A7%C3%A3o?utm_source=chatgpt.com)

**4. Vulnerabilidades exploradas:** Foram exploradas quatro vulnerabilidades zero-day, incluindo:​

* CVE-2023-38606 (falha no kernel do iOS)​[Wikipédia, a enciclopédia livre](https://pt.wikipedia.org/wiki/Opera%C3%A7%C3%A3o_Triangula%C3%A7%C3%A3o?utm_source=chatgpt.com)
* CVE-2023-41990 (falha no mecanismo de processamento de fontes FontParser)​[Wikipédia, a enciclopédia livre](https://pt.wikipedia.org/wiki/Opera%C3%A7%C3%A3o_Triangula%C3%A7%C3%A3o?utm_source=chatgpt.com)

**5. Impactos e/ou prejuízo:** O ataque afetou milhares de dispositivos, incluindo os de organizações comerciais, governamentais e diplomáticas. A espionagem resultou na exposição de informações sensíveis e comprometeu a segurança de dados pessoais e corporativos.​[Wikipédia, a enciclopédia livre](https://pt.wikipedia.org/wiki/Opera%C3%A7%C3%A3o_Triangula%C3%A7%C3%A3o?utm_source=chatgpt.com)

**6. Tipo de proteção que poderia ter sido aplicada:** Atualizações regulares do sistema operacional para corrigir vulnerabilidades conhecidas, uso de soluções de segurança móvel que detectem comportamentos anômalos, restrições no recebimento de mensagens de remetentes desconhecidos e conscientização dos usuários sobre os riscos de ataques direcionados.